

**TEST AND EVALUATION MASTER PLAN (TEMP)  
FOR  
GLOBAL COMMAND AND CONTROL SYSTEM V3.0**

**2 September 1997**

**PREPARED BY**

\_\_\_\_\_  
Program Manager

\_\_\_\_\_  
DATE

**SUBMITTED BY**

\_\_\_\_\_  
Program Director

\_\_\_\_\_  
DATE

**CONCURRENCE**

\_\_\_\_\_  
Joint Interoperability Test Command

\_\_\_\_\_  
DATE

\_\_\_\_\_  
User Representative (Joint Staff-J33)

\_\_\_\_\_  
DATE

**OSD APPROVAL**

\_\_\_\_\_  
Deputy Director, Operational Test  
& Evaluation, OSD

\_\_\_\_\_  
DATE

\_\_\_\_\_  
Deputy Director, Developmental Test  
Systems Engineering & Evaluation,  
OSD

\_\_\_\_\_  
DATE

# GLOBAL COMMAND AND CONTROL SYSTEM 3.0 TEST AND EVALUATION MASTER PLAN

## TABLE OF CONTENTS

### **PART I SYSTEM INTRODUCTION**

1.1 Mission Description.....	I-1
1.2 System Threat Assessment .....	I-2
1.3 Measures of Effectiveness and Suitability.....	I-2
1.4 System Description.....	I-7
1.4.1 Functional Capabilities .....	I-8
1.4.1.1 C4I Capabilities .....	I-8
1.4.1.2 JOPES.....	I-8
1.4.1.3 Mission Support Applications .....	I-8
1.4.1.4 Common Operational Environment.....	I-8
1.5 Critical Technical Parameters.....	I-12

### **PART II INTEGRATED TEST PROGRAM SUMMARY**

2.1 Integrated Test Program Schedule .....	II-1
2.1.1 Critical System Milestones .....	II-3
2.2 Management.....	II-4
2.3 Procedures .....	II-9

### **PART III DEVELOPMENTAL TEST AND EVALUATION**

3.1 Modified Developmental Test and Evaluation Overview .....	III-1
3.2 Developmental Test and Evaluation to Date .....	III-8
3.3 Future Modified Developmental Test and Evaluation.....	III-9

### **PART IV OPERATIONAL TEST AND EVALUATION OUTLINE**

4.1 Operational Test and Evaluation Overview .....	IV-1
4.2 Critical Operational Issues .....	IV-3
4.3 Operational Test and Evaluation to Date .....	IV-5
4.4 Future Operational Test and Evaluation.....	IV-6
4.4.1 MDT Support of OT.....	IV-6
4.4.2 Transition Test.....	IV-6
4.4.3 Training, Documentation, and User Support Test.....	IV-7
4.4.4 Simulated Crisis Situation Exercise .....	IV-9
PART IV APPENDIX - Mission Tasks and Mission Support Tasks .....	IV-11

### **PART V TEST AND EVALUATION RESOURCE SUMMARY**

5.1 Test and Evaluation Resource Summary.....	V-1
---	-----

## **APPENDICES**

APPENDIX A - Glossary.....	A-1
APPENDIX B - System Interfaces .....	B-1
APPENDIX C - References.....	C-1
APPENDIX D - GCCS v3.0 Functionality.....	D-1
APPENDIX E - Year 2000 Certification Plan.....	E-1
APPENDIX F - Considerations for Future Assessment.....	F-1

## **LIST OF FIGURES**

Figure II-1 GCCS Program Schedule .....	II-1
Figure III-1 GCCS 3.0 Developmental Test and Evaluation Events .....	III-2
Figure IV-1 GCCS Version 3.0 OT&E Strategy .....	IV-2

## **LIST OF TABLES**

Table III-1 MDT&E Exit Criteria.....	III-3
Table III-2 MDT Products .....	III-7
Table III-3 GCCS Future Developmental Test and Evaluation Events.....	III-9
Table 1 CAP Phases .....	IV-11
Table 2 Mission Tasks, Crisis Action Planning Matrix, Phase I .....	IV-13
Table 3 Mission Tasks, Crisis Action Planning Matrix, Phase II .....	IV-14
Table 4 Mission Tasks, Crisis Action Planning Matrix, Phase III.....	IV-15
Table 5 Mission Tasks, Crisis Action Planning Matrix, Phase IV.....	IV-18
Table 6 Mission Tasks, Crisis Action Planning Matrix, Phase V .....	IV-19
Table 7 Mission Tasks, Crisis Action Planning Matrix, Phase VI.....	IV-21
Table 8 Additional Mission Tasks.....	IV-22
Table 9 Mission Support Tasks .....	IV-25
Table V-1 Operational Test (OT) Personnel Requirements .....	V-2

## **PART I**

### **SYSTEM INTRODUCTION**

#### **1.1 Mission Description**

a. This Test and Evaluation Master Plan (TEMP) applies to the Global Command and Control System (GCCS) Version 3.0 capabilities leading up to and including the replacement of the current version of GCCS. This includes version 2.2 and subsequent versions of 2.2.n software releases. This TEMP will be updated to reflect incremental improvements/upgrades of GCCS v3.0 as necessary.

b. The J3 approved GCCS Mission Needs Statement (MNS) identifies the objectives for GCCS as those identified in the Defense Planning Guidance, Section III, "Command, Control, Communications, Computers, and Intelligence (C4I) and Space Base Systems." Planning guidance for the GCCS is also contained in DODI 4630.8 and the Joint Chiefs of Staff "C4I for the Warrior (C4IFTW)" concept and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01. The GCCS MNS is intended to be one of several MNS within the C4IFTW concept. The GCCS mission requirements are further specified in a Requirements Implementation Document (RID) and an Evolutionary Phase Implementation Plan (EPIP).

c. The GCCS MNS states the required need for selected common functionality among the combatant commands, Services, and agencies which will allow interconnecting to the theater and task force level communications infrastructures. Details of implementation are found in the GCCS Concept of Operations (CONOPS). The mission need is to support the warfighter with information tools to enable effective and timely accomplishment of the mission. GCCS is the automated tool for the warfighter which satisfies that need. GCCS integrates national, theater, and tactical information into a common, fused picture of the battle space for the warfighter.

d. The Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (ASDC<sup>3</sup>I) has approved GCCS as the Command and Control migration system for all the Commanders in Chief (CINCs) and Services/Agencies. The Under Secretary of Defense (Acquisition) (UDS(A)) terminated the World Wide Military Command and Control System (WWMCCS) in August 1996, when GCCS became the C2 System Of Record (SOR). GCCS performs not only the many functions of WWMCCS, but also achieves additional functionality required by the Warfighter in a common and interoperable way.

e. GCCS 3.0 will provide the National Command Authorities (NCA) with an infrastructure that will effectively control the flow and processing of information to implement command and control over our national agencies, military forces, and allies throughout the force projection cycle. This capability will extend from the NCA to the CINCs; between the supported and supporting CINCs; from the supported CINC to the Commander Joint Task Force (COMJTF); and from the COMJTF to the component commands. GCCS 3.0 will facilitate the ability of the warfighter to perform deliberate planning, crisis planning, execution, follow-on operations, and peacetime operations.

## **1.2 System Threat Assessment**

The Joint Staff will conduct the Threat Assessment for the GCCS and provide that document separately.

## **1.3 Measures of Effectiveness and Suitability (MES)**

The RID, EPIP and the CONOPS constitute the complete requirements documents validated by the Joint Staff. These MES were used to determine the Critical Operational Issues (COI) discussed in section IV of this document:

a. Interoperability. GCCS must interface with Service and site unique systems which pass data to/from GCCS. The GCCS interface requirements draft provided by Joint Interoperability Test Command (JITC) is found at Appendix B.

b. Security. The Security Test and Evaluation (ST&E) will be performed in order to accredit GCCS v3.0 to operate at the Secret level. (Reference CJCSI 6731.01 GCCS Security Policy, the GCCS Automated Information System Security Plan, and associated security documentation). All GCCS v3.0 delivered software should meet the security requirements identified within the Trusted Facility Manual (TFM). The results of the ST&E will be used to definitize the security Critical operational Issue (COI 3) and addressed as part of the overall evaluation of GCCS v3.0. The ST&E will assess how vulnerable GCCS is from an IW perspective and the accreditation report following from the ST&E will discuss the assessments and factors in risk mitigation for each of the vulnerabilities discussed.

c. Collaborative access to a common Operations Plan (OPLAN). GCCS must support collaboration between the theater-level Joint Operation Planning and Execution Community (JPEC) combatant commands, supported and supporting commanders, agencies, Service components, the CJTF and subordinates. GCCS must provide visibility of plan execution status at all levels of command. The specific processes that must be supported include:

- Courses of Action (COA) development
- Forces and task refinement
- Employment analysis
- Specialized employment analysis (e.g., employment of special capabilities that may not currently be in the theater)
- Deployment/transportation analysis
- Sustainment analysis
- On-line refinement teleconferencing
- Remote briefing
- Tailored plan dissemination
- Re-deployment

d. Performance. GCCS Version 3.0 system performance must meet or exceed GCCS v2.2 performance standards. Success will be determined by subjective user assessment.

## **1.4 System Description.**

a. GCCS v3.0 is being fielded as the baseline system representing the objective functionality of the Global Command and Control System capability. It will replace several earlier fielded versions and incorporate the Defense Information Infrastructure Common Operating Environment (DII COE), the Common Desktop Environment, update the Oracle relational data base management system and add new functionality to the current GCCS v2.2. The fielding strategy is to accomplish this in a series of incremental fieldings. To minimize risk and time, the current GCCS v2.2 functionality will be ported to the new operating environment in the initial release. Subsequent releases will add improved functionality as new applications are released by the Defense Information Systems Agency (DISA). As a product improvement, the additional releases will not necessitate a revised TEMP and may not require full testing.

b. GCCS is the primary joint command, control, communications, computer and intelligence systems for the United States Department of Defense (DOD) and provides an integrated architecture of communications and information processing systems capable of responding to military contingencies worldwide. GCCS v3.0 utilizes applications developed by many formal acquisition programs to provide an integrated capability at most levels of command. GCCS is a "system of functionalities" using a common database. It uses a client-server architecture with commercial off-the-shelf (COTS) hardware and the Defense Information Infrastructure Common Operating Environment (DII COE) to achieve consistent operation across multiple platforms. Core functions and applications software packages will be selected from migration candidates satisfying selection criteria proposed by the GCCS Program Manager and approved by the GCC Advisory Board IAW CJCSI 6721.01, Global Command and Control Management Structure and the GCCS Functional Requirements Evaluation Procedures.

c. The GCCS software and hardware configuration, with detailed installation and administration instructions, is described in the GCCS version description, GCCS system administration manual and GCCS implementation procedures documents. The configuration identified in the GCCS administration instruction describes the GCCS configuration which will be used for testing. During testing, the configurations of all test sites will be placed under strict configuration management (CM) by the local CM groups and a joint test team composed of both users and testers.

d. The backbone communications for GCCS is the Defense Information System Network (DISN). The DISN is a collection of voice and data networks composed of multiplexers, cryptographic devices, routers, and other devices combined to create a world wide information transfer infrastructure. One of the data portions of the DISN is comprised of router based layers, each with a different classification level. The secret router layer is the Secret Internet Protocol Router network (SIPRNET). The GCCS premise router is part of the GCCS site Local Area Network (LAN) infrastructure and represents the gateway point out to the SIPRNET Wide area Network (WAN). Communications servers support access to GCCS via Secure Telephone Unit (STU) using dial or dedicated multiplexer circuits.

e. There will be a transition period during which older versions of GCCS v2.2 will operate at some sites while version 3.0 will operate at others. Care will be taken to insure that a logical transition plan is enacted whereby GCCS v3.0 servers which can be accessed by GCCS v2.2 clients are installed first. This will insure uninterrupted GCCS service since GCCS v2.2

clients can operate with GCCS v3.0 servers, but version 3.0 clients can not operate with version 2.2 servers.

f. The functionality for GCCS Version 3.0 is described in the GCCS Version Description Document (VDD) and was selected in accordance with Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6721.01. The GCCS user CONOPS document defines eight objectives for GCCS. These objectives are:

1. Be configurable to achieve optimum crisis response.
2. Support unity of effort and command dominance.
3. Support deliberate and crisis action planning.
4. Provide for joint operations Time Phased Force Deployment Data (TPFDD) development and updating.
5. Provide Combined Joint Task Force (CJTF) global access to current intelligence and tactical information, in support of joint and coalition missions.
6. Support decision and execution cycles faster than those of any enemy.
7. Provide interoperability for joint and multinational force Command and Control (C2) systems.
8. Facilitate use of Commercial Off The Shelf (COTS) products.

#### **1.4.1 FUNCTIONAL CAPABILITIES.**

GCCS Version 3.0 will provide the capabilities described in the draft GCCS Version 3.0 CONOPS, sections III and IV, in the GCCS MNS, and Annex C to the GCCS 3.0 EPIP (Functional Description), June, 1997, where specific segment descriptions are grouped by Solaris, HP, and NT platforms. GCCS capabilities are allocated to four broad functional areas. These functional areas and their respective applications are:

**1.4.1.1 C4I Applications.** GCCS v3.0 applications support a span of control from threat assessment and force requirements development through lift, deployment, sustainment and return. The integration of various intelligence sources and communications links provides the entire GCCS community with an integrated representation of the battle space. C4I applications include:

- a. Automated Message Handling System (AMHS)
- b. Common Operational Picture (COP)
- c. GCCS Air Tasking Order (ATO) Review Capability (GARC)
- d. Global Reconnaissance Information System (GRIS)

- e Global Status Of Resources and Training System (GSORTS)
- f. Global Transportation Network (GTN)
- g. Joint Deployable Intelligence Support System (JDISS)

**1.4.1.2 Planning and Execution Applications. Joint Operation Planning and Execution System (JOPES)** Time Phased Force and Deployment Data (TPFDD) is used to develop plans and alternatives, as well as the execution of approved plans. In addition to the tools listed below, GCCS v3.0 must maintain synchronization of the JOPES core database content across database sites.

- a. Requirements Development and Analysis (RDA)
- b Scheduling and Movement (S&M)
- c Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE)
- d Joint Flow and Analysis System for Transportation (JFAST)
- e Joint Engineer Planning and Execution System (JEPES)
- f Ad Hoc Query (AHQ)
- g Information Resource Management (IRM)
- h Pre-defined Reports (PDR)
- i Joint Planning and Evaluation Toolkit (JPET)
- j Joint Forces Requirements Generator (JFRG)

**1.4.1.3 Mission Support Applications.** GCCS, Version 3.0 currently provides the following mission support applications, listed below. As the Department of Defense (DoD) mission support applications are integrated into the DII, they will become available to GCCS users, as appropriate.

- a. Airfields
- b. Evacuation File Maintenance and Retrieval System (EVAC)

**1.4.1.4 Common Operating Environment (COE) Support Applications** COE Support Applications provide the following user services, listed below. The primary objective is to furnish generic, COTS based information transfer services to the GCCS user community and their applications.

- a. Office Automation

- b. Teleconferencing
  - (1) Internet Relay Chat (IRC)
  - (2) Internet News
  - (3) World Wide Web (WWW)
  - (4) e-mail
- c. TELNET
- d. File Transfer Protocol (FTP)

### **1.5 Critical Technical Parameters**

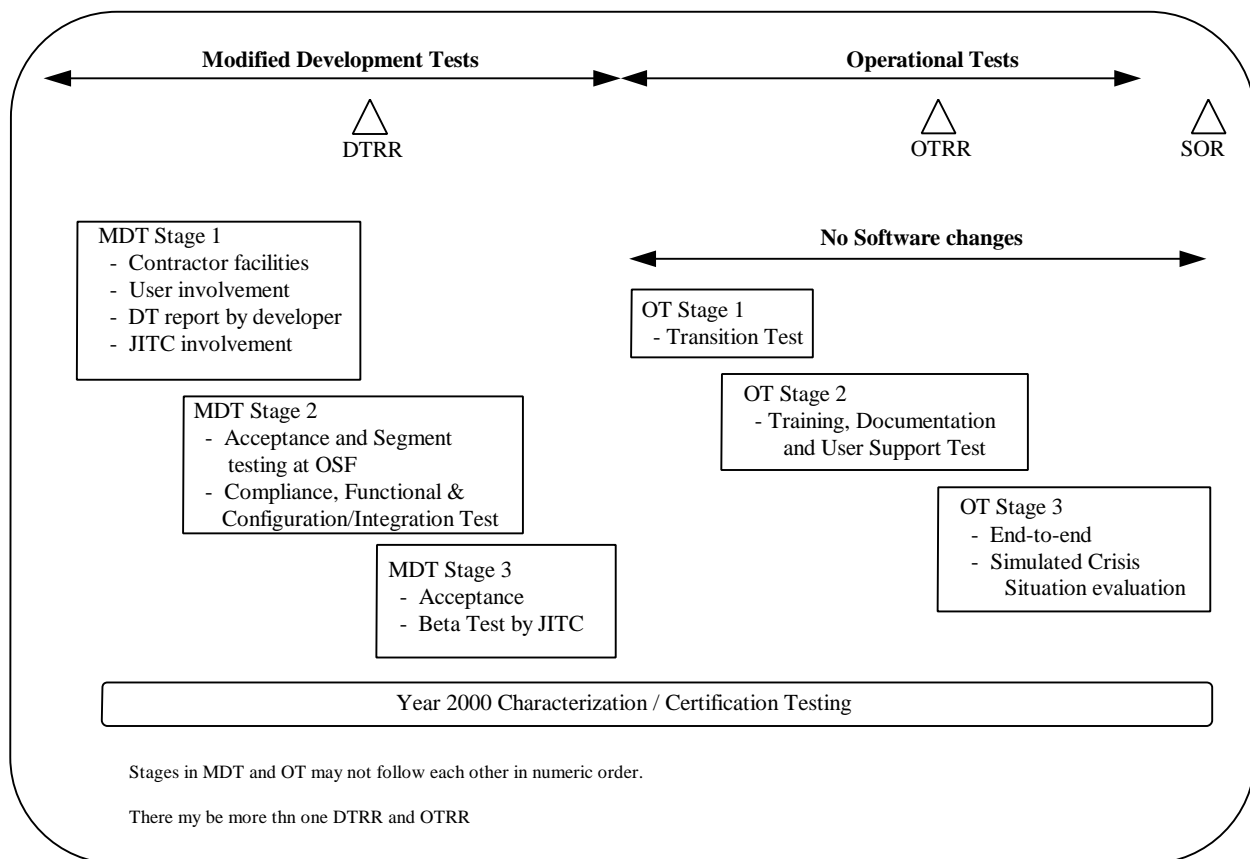
The GCCS contains several independently developed software components which collectively comprise the system. For that reason, the GCCS contains no system level critical technical parameters (CTP). Specific CTP for the components of GCCS will be application specific. These parameters are defined and published for specific applications.

## PART II

### INTEGRATED TEST PROGRAM SUMMARY

#### 2.1 Integrated Test Program Schedule.

This section identifies overall responsibilities for managing, conducting and coordinating GCCS test activities. Figure II-1 identifies the key events and activities to support the testing, evaluation, and fielding of GCCS Version 3.0. The GCCS Program Management Plan describes a time-phased implementation approach for overall GCCS program management and implementation. As stated in paragraph 1.4, GCCS will be fielded in increments starting with the porting of current GCCS v2.2 functionality to the new operating environment. Improved functionality will be integrated as it becomes available. The GCCS test and evaluation strategy is designed to leverage the development and integration efforts of a large number of programs. Each program may have several development organizations. GCCS includes CINC and Service feeder applications which must be integrated before GCCS user exercises can be run. In addition, new applications will be integrated as they become available. GCCS will employ an incremental integration, test and fielding approach. Target application requirements identified by the functional proponent will be segmented, tested, and fielded. The Test and Evaluation (T&E) strategy will utilize developmental and operational test and evaluation methods described in parts three and four of this TEMP, respectively.



**Figure II-1 GCCS Program Schedule**

a. Development Test & Evaluation. A Modified Development Test (MDT) approach will be used for GCCS Version 3.0 that includes the stages described below:

MDT Stage 1 will be conducted at the developer's facilities. The GCCS functional users will assist the contractor in evaluating the functionality with demonstrations and testing before delivery. JITC will provide oversight and will provide reports during this testing to the GCCS Program Office. The developer will provide a DT Report prior to delivery of the components to the Operational Support Facility in the formal segment delivery process.

MDT Stage 2 will be conducted at the Operational Support Facility. This Stage will include compliance, functional and configuration/integration testing of the initial component deliveries. System builds and installation instructions will be validated. GCCS Software Problem Reports (GSPR) fixes will also be validated in Stage 2.

MDT Stage 3 will be led by the JITC and consist of a beta test with user involvement and acceptance as part of OT Readiness Review. This stage will include a test of the compatibility of GCCS v2.2 and version 3.0 systems.

b. Operational Test & Evaluation. Operational Test & Evaluation (OT&E) will be performed by the JITC in conjunction with the Service Operational Test Agencies (OTA) (AFOTEC, OPTEC, OPTEVFOR, MCOTEA). Operational assessments of the earlier versions of GCCS were conducted by the user community under the auspices of the Joint Staff (J3). Additional assessments of CINC and Service feeder applications integrated into GCCS 3.0 will be performed by the providing CINC or Service, and supplemented by independent operational tests. An Operational Test Readiness Review (OTRR) will be convened to determine the suitability of the system to enter operational testing. The OTRR will establish the 3.0 baseline. Once OT has commenced, no major software changes will be permitted without returning to MDT. The OT will be conducted in three stages which may start and overlap in any order. The stages of the OT are described below:

OT Stage 1, Transition Test. JITC will conduct the Mission Support Test at multiple operational sites. The objective is to determine if mission support technical personnel (for example, system administrators, database administrators, network administrators, security personnel) can install and configure the system, migrate user accounts and data from the GCCS v2.2 to v3.0 formats and account management system, establish user permissions, establish network connectivity, establish security controls, and otherwise prepare the system for effective operation. The GCCS user community will provide subject matter experts (SMEs) to support assessment of Mission Support task success. The criteria to be used for assessment of compatibility are whether 2.2 clients can access either 2.2 or 3.0 servers, and whether 2.2 and 3.0 clients can be easily pointed to alternate 3.0 servers. OT compatibility testing will continue efforts of MDT.

OT Stage 2, Training, Documentation and User Support evaluation. This stage will not include structured test activities. JITC will review the training program, system documentation, and procedures for user support. JITC may support the assessment by administering questionnaires to selected user personnel. The objective is to determine if the training is adequate to prepare the users to perform their missions, if the documentation is adequate for use by operational personnel,

and if the user support structure (for example, help desk) is adequate for operational use.

OT Stage 3, Simulated Crisis Situation. JITC will conduct this test, to the maximum extent possible, at multiple operational sites (and, possibly, one or more lab sites). Functionally, it is desired that the sites represent a supported CINC, one or more supporting CINCs, the NMCC or its surrogate, a Joint Task Force (JTF) headquarters (austere environment), and an afloat headquarters. Actual users will operate the system at all sites (including any lab sites). The GCCS user community will provide subject matter experts (SMEs) to verify successful operation of GCCS applications.

c. Year 2000 (Y2K) Certification. JITC will determine Y2K compliance and certification in conjunction with many assessment, test, and auditing activities. The basis of the certification will include: Government risk assessments performed on all GCCS developer's methodology, Developer's testing results, Integrated Developmental/Operational testing (DT/OT) results, and specific JITC-designed Y2K checks. The certification process builds from assessments and results, ensuring that Y2K engineering and management attention are committed throughout the process. Each building block increases the confidence level leading to system certification. Results and issues will be identified and tracked to resolution. Results, assessment and JITC experience will form the basis for certification. Detailed information is provided in the Year 2000 Certification Plan, Appendix E.

### **2.1.1 Critical System Milestones.**

a. The milestones listed here are not accompanied by dates due to the uncertain nature of the precise test schedule.

- (1) Deliver test peculiar hardware to DT sites
- (2) Deliver software to DT sites
- (3) Conduct Stage III MDT
- (4) OTRR 1
- (5) OTRR 2
- (6) Deliver software to OT sites
- (7) Correct software anomalies found in MDT
- (8) Conduct functional OT
- (9) Conduct installation OT
- (10) SOR decision

b. Sufficient written procedures and documentation available to the user including:

- (1) Application user manuals
- (2) Training manuals (for system, security, database, and network administrators)
- (3) Integrated Logistics Support Plan (ILSP)
- (4) Administrative Documents (EPIP, Operational Test Plan, and CONOPS)
- (5) Detailed system documentation for systems administrators. This includes
  - (a) Contents of the new load: what is the file laydown, what files and directories are created and written to by the load process, and what files get overwritten.

(b) Server configuration information: file system size estimates/minimums; expected NFS mounted file systems; extent of TFM compliance. DISA must clearly identify any files, structures, etc. that must be set or re-set at the site.

(c) Individual application details: application name; developer; short functional description; software run requirements; directories (what files are being placed in which directories); Lists of software on clients and on servers; initiating sequence; sequence of launch events; icon bitmap files; names of source files; what are the user-configurable files for the application; What system-level variables are being set by each application; Does the application rely on remote shelling for execution; Does the application reference alias host names; Dependency chart between applications, i.e., How application affects or uses information from other applications (tables being updated, files being replaced, CPU requirements/effect of a CPU-bound process on other applications and on itself when it has less than its optimum CPU share)

(d) List of system and application/segment default settings: when a particular application is installed, does the installation overwrite the current account configurations. Some applications have user- or SA-configurable flat files. If default settings are documented, SA's will be able to re-configure for the new version.

(e) Account migration process for 2.2 user accounts, authorizations, privileges, and data. This account and data migration will be the driving factor in the resulting downtime from the users' perspective.

The description should include the following areas:

(1) Pseudo-code demonstrating how the migration process from v. 2.2 to 3.0 handles the range of account folders (personal and shared folder types: project, position, directorate, division, branch, section, cell), all of which are under the shared global folder directory.

(2) Advance notification and description of the amount of manual labor in account and data migration.

(f) Description of the new login access mechanism and account management mechanism.

(g) Description of Installer.

(h) Database Entity Relationship Model/Diagram and Data Dictionary.

## **2.2 Management.**

Management responsibilities for the GCCS program are as follows:

a. Director, Operational Test and Evaluation (DOT&E). Responsible for the final approval of coordinated TEMP and Operational Test and Evaluation Plan (OTEP). Also responsible for the oversight of test planning and conduct and independent evaluation and reporting of GCCS performance.

b. Director, Test, Systems Engineering and Evaluation (DTSE&E). Reviews development test results to analyze residual risks and satisfaction of DT exit criteria.

c. Joint Staff. Responsible for the following activities:

- (1) The specification and approval of operational requirements.
- (2) Conducting a threat assessment for GCCS.
- (3) Approving exit criteria at each stage of MDT and OT.
- (4) Coordinating user and/or SME support as necessary.
- (5) Validating any modifications or interpretations of the user requirements. This may require approving changes to the operational requirements.
- (6) Final approval authority for the operational use of GCCS v3.0.
- (7) Providing test scenarios as needed.
- (8) Represent the CINCs for the TEMP and OTEP.
- (9) Establish user Concept of Operations (CONOPS).
- (10) Preparing the type accreditation for GCCS.

d. The GCCS Program Management Office (PMO) has responsibilities for the following activities:

- (1) Ensuring testers and functional users and site technical support staffs have access to developer and DISA facilities, products and data.
- (2) Ensuring MDT and OT efforts are adequately resourced (in a timely manner).
- (3) Interfacing with the Joint Staff, CINC, Service and Agency (C/S/A) users to ensure all requirements are considered. Requirements will be validated IAW the GCC management structure.
- (4) Resolving conflicts between C/S/A functional user, technical support staff and developer, if any. This specifically addresses contract deliverables and meeting user requirements.
- (5) Completing and coordinating the TEMP.

e. DISA/JIEO/OSF. Responsible for the following activities:

- (1) Complete the description of the transition strategy options for fielding and backing up the GCCS both before and after GCCS v3.0 SOR. DISA will provide version description documents, system administration procedures and a cutover

plan for the database and long haul communications. Detailed systems documentation for site system administrators will include those items listed in para 2.1.1b(5) above.

- (2) Provide baseline and developmentally tested software and related support to GCCS fielding sites.
- (3) Complete the development test of the DII Common Operating Environment (COE).
- (4) Ensure the capability to restore GCCS v2.2 to full operation.
- (5) Validating installation procedures as defined in the engineering strategy.
- (6) Validating COE compliance and providing results to developer.
- (7) Testing baseline software and publishing emerging results.
- (8) Using applicable metrics to evaluate the status of the system.
- (9) Providing overall system status reports in coordination with the JITC.
- (10) Participating in MDT and OT as a supporting test node.
- (11) Retesting GSPRs and providing results to the Joint staff.

f. Services. Responsible for the following activities:

- (1) The specification and approval of the operational requirements and operational procedures for Service unique elements of GCCS
- (2) Conduct operational test and evaluation for GCCS Service Interfaces and Service unique mission critical capabilities in support of the OTEP and appended Service test plans. Operational test support includes writing test plans, test execution, evaluating test results and providing the evaluation of operational effectiveness and suitability to JITC for consolidation into the overall GCCS evaluation. This will allow JITC to monitor Service unique testing prior to System of Record (SOR).
- (3) Provide GCCS v3.0 cut-over recommendations to Joint Chiefs of Staff (JCS)/J3.
- (4) Conduct Y2K compliance checks and results for service-unique interfaces. Support GCCS Y2K certification process.

g. JITC. Responsible for the following activities:

- (1) Establishing an Independent test team.
- (2) Identifying and verifying testable GCCS 3.0 requirements.
- (3) Recommending applicable software metrics for GCCS 3.0.
- (4) Coordinating input to test documentation for MDT stages 1 and 2.
- (5) Producing test documentation.
- (6) Coordinating with Joint Staff, GCCS functional area working groups, and C/S/A communities to ensure user interest.
- (7) Recommending areas for functional and technical SME assessments/involvement.
- (8) Reviewing applicable system documentation to include detailed system documentation listed in para 2.1.1b(5) above.
- (9) Providing emerging results reports as applicable and providing a system status report at the end of each stage of testing.
- (10) Developing the test scenario and steps/cases for MDT Stage 3 and OT.
- (11) Providing anomaly reports.
- (12) Providing requirements assessment.
- (13) Providing test report with recommendations.
- (14) Interfacing and coordinating with DISA security personnel for GCCS security issues.
- (15) Drafting appropriate entrance and exit criteria for each stage.
- (16) Coordinating with the PMO to produce Parts III and IV of the TEMP.
- (17) Providing input to Parts I and II of the TEMP.
- (18) Independent operational testing.
- (19) Interoperability testing and certification, to include Year 2000 (Y2K) testing.
- (20) Coordination with Service test communities to leverage test planning, conduct, and evaluation of Service-unique critical mission tasks.

- (21) Coordinate user involvement at the contractor facilities for the purpose of operational assessment.
- (22) Site installation evaluation.
- (23) Consolidating the reporting of entrance and exit criteria requirements.
- (24) Writing the OTEP and serving as the single operational test integration point of contact.
- (25) Test training and coordination.
- (26) Control over the GCCS configuration during the operational stage of testing, and control over access by contractors that might alter the configuration or otherwise influence the results of operational testing.
- (27) Ensure that all mission critical tasks are performed and evaluated, or that the consequences of not performing any critical mission are assessed by the affected functional users as an acceptable risk and test limitation.
- (28) Consolidate evaluation reports from appropriate sources; conduct, analyze, and evaluate the joint portion of GCCS operational testing; and report test results directly and simultaneously to the Joint Staff, Director of DISA, and DOT&E with information to the Services.
- (29) Consolidate Y2K assessments and test data from appropriate sources; test, assess and evaluate GCCS for certification and report conclusions directly to the Joint Staff, Director of DISA, and DOT&E with information to the Services.

h. CINCs, Services and Subject Matter Experts (SMEs). Responsible for the following activities:

- (1) Providing experienced and knowledgeable functional and technical user representatives as the designated SME - the primary interface for specific GCCS components/ applications.
- (2) Monitoring Newsgroups that are announcing problem report fixes.
- (3) Responding to scheduled opportunities to visit developers and to participate in functional user demonstrations of their designated GCCS functional components/applications.
- (4) Providing input to the MDT and OT teams to help develop appropriate software metrics and performance benchmarks for their specific GCCS component/application.
- (5) Reviewing plans for and participating in the integration, configuration, and

systems tests conducted at the oPERATIONAL sUPPORT FACILITY (OSF).

(6) Reviewing plans for and participating in the network and systems tests conducted at designated Beta test sites, the JITC, or the Joint Development and Evaluation Facility (JDEF).

(7) Reviewing detailed system documentation provided by DISA in order to facilitate site configuration and troubleshooting. (technical support staff only—SA's, DBA's, etc.)

(8) Assist the OT&E test team in identifying critical activities to evaluate and to determine the operational implications of test incidents during testing.

### **2.3 Procedures**

a. Adjudication. Problems identified by exception during testing will be adjudicated by on-site teams consisting of users and administration personnel as selected by the sites. The adjudication process compensates for a lack of required or well defined performance standards and allows functional users and site technical support staff to determine criticality of incidents. During designated test periods, the adjudication process will determine scoring of test incidents prior to forwarding the test incidents to the JITC for collection and analysis. Certain categories of problems will require the submission of both the test incident form as well as a GCCS System Problem Report (GSPR) through established channels to the Program Manager. In these cases, the test incidents form will include a cross-reference to the GSPR submission.

b. Test Independence. The test team members must be independent from the system developers and integrators. Test results need to be consolidated and reported through independent channels rather than user or developer channels. Users in the test must be able to express themselves freely.

## PART III

### MODIFIED DEVELOPMENTAL TEST AND EVALUATION

#### 3.1 Modified Developmental Test and Evaluation (MDT&E) Overview

The MDT&E effort for GCCS will verify the status of engineering development progress within each segment, verify that design risks have been minimized, substantiate achievement of technical performance requirements, measure the effectiveness of the functional requirements and certify readiness for operational test (OT) through use of SW Metrics and MDT results and analysis.

- a. DT&E Test Philosophy. GCCS will use a modified DT&E test philosophy that incorporates the following concepts:

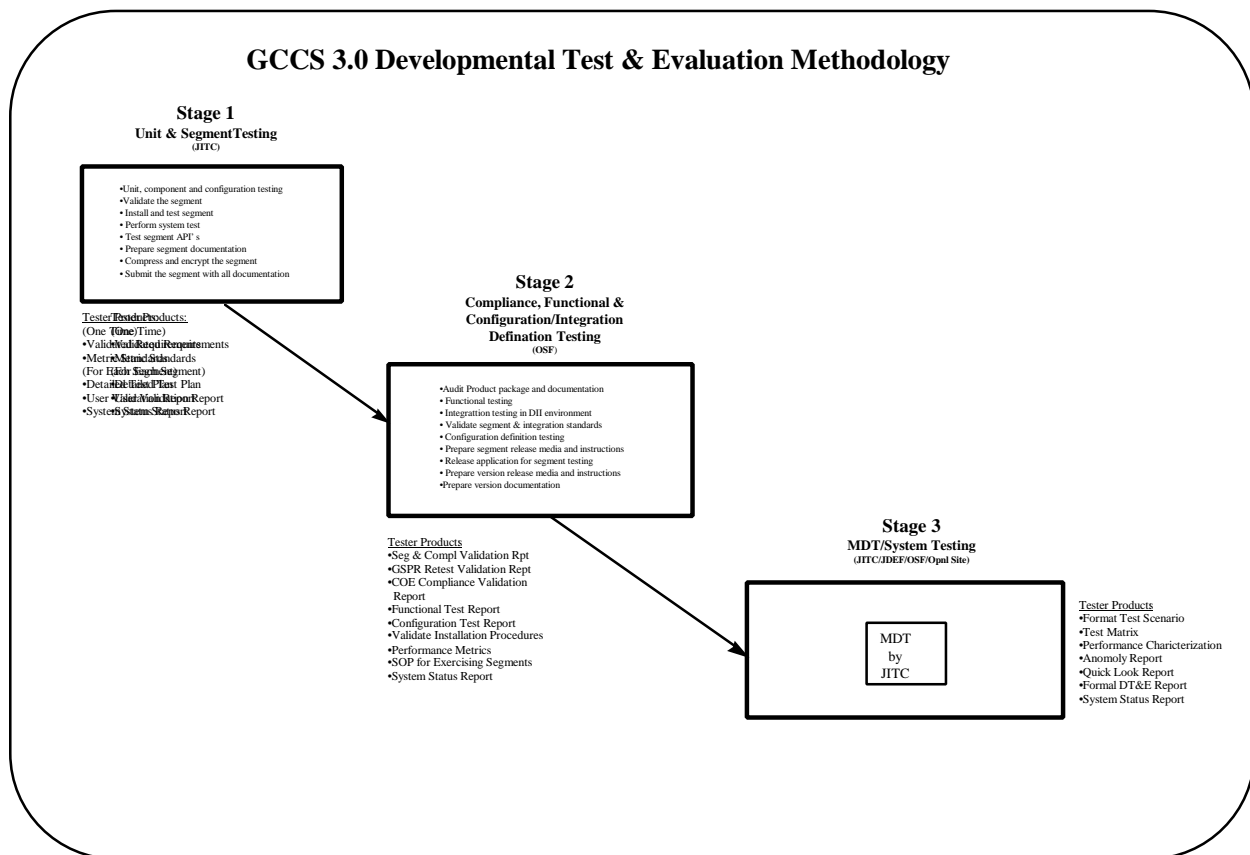
- (1) Stronger user involvement. Early involvement from the functional user community is the key to a successful MDT approach. Working closely between the developers and user community in developing GCCS capabilities helps ensure functional requirements are met and capabilities can be evaluated in a user-oriented environment.
- (2) Extensive use of existing software. GCCS will integrate a wide assortment of software systems that interface in a standard way with the DII COE. The applications to be integrated include existing command and control systems, and systems created and used by the Services. One of the goals of GCCS is to fully integrate selected Service applications that use the DII COE, to avoid large and lengthy development efforts.
- (3) Use of event driven scenarios based on requirements as a means of evaluating the effectiveness of GCCS products and application software in a user-oriented environment.
- (4) Use of exercise-like scenarios during end-to-end testing to evaluate the effectiveness of the multi-node environment and benchmark the thresholds of the system. New versions will be at least as capable in performance as the version replaced.
- (5) Customizing the test and evaluation process according to segment type and the magnitude of the risk involved with inserting the segment into the operational GCCS system. Because the GCCS is made up of applications developed by each of the Service components, as well as COTS software, the testing completed by the development activity will be factored into the independent MDT&E activities.
- (6) Use SW Metrics throughout the development effort to measure the growth and stability of the GCCS system. These metrics will provide a portion of the entrance criteria into the OT&E effort as well as provide a “snap shot” of the current status of the GCCS system.

(7) Ensure that the OT&E interests are considered during MDT&E events to include the participation of the OT&E community at MDT planning events, MDT events and MDT analysis and reporting efforts.

(8) Use of development test data by the operational test community as preliminary operational data for input into their assessments supporting GCCS Version 3.0 determination of operational effectiveness and suitability and minimizing the need for collecting data multiple times.

(9) Ensure Year 2000 (or suspected Year 2000) issues are reported to appropriate program and test managers.

b. DISA Developmental Test and Evaluation Methodology. The objectives of DISA developmental test and evaluation for GCCS are to reduce the risk of adverse impacts when inserting new segments and technology into the operational system, and determine the effectiveness and supportability of the component in a user-oriented environment. DISA will oversee and conduct MDT for the GCCS Version 3.0 development and integration effort prior to Operational Test and Evaluation (OT&E) efforts. The MDT&E methodology incorporating the MDT&E philosophy into a three staged MDT approach is depicted in Figure III-1 below and detailed in subsequent paragraphs within this section. The following paragraphs describe the MDT&E methodology for GCCS version 3.0. Table III-1 list the exit criteria for each of the three MDT stages and Table III-2 list the products for each stage of MDT.



**Figure. III-1. GCCS 3.0 Developmental Test & Evaluation Methodology**

(1) **Application and Segment Testing**. Stage 1 encompasses Unit and Segment Testing conducted at the developer's facilities. The segments or units will be developed and documented in accordance with MIL-STD-498, the segments shall be validated with their appropriate platform COE and user participation for applicable segments will be required. JITC will provide oversight and guidance to the developer to ensure exit criteria, shown in Table III-1 from Stage 1 have been met and SW Metrics are captured to effectively measure Stage 1 events.

**Table III-1. MDT&E Exit Criteria**

<b>Stage 1 Application &amp; Segment Testing</b>	<b>Stage 2 Compliance and Integration Testing</b>	<b>Stage 3 MDT/System Testing</b>
Application functionality verified at developer facility	Application functionality verified at Government facility	Application/System functionality verified at lab and operational sites
High priority GSPRs fixed, adequate workaround documented, or program decision on GSPR is made.	Scheduled GSPR fixes are validated in lab; OSF integration and unit testing performed	Scheduled GSPR fixes validated by user
	Segments are Validated for DII COE Compliance in the lab	Installation instructions are verified by functional and technical user
	Installation Instructions are verified in lab	Compatibility with latest 2.2 release

a. The Designated Development Agency (DDA) for all segments and major configuration items will complete a Formal Qualification Testing (FQT) process in accordance with MIL-STD 498 during unit and segment testing. A Software Test Plan (STP) will document the developer's plans for conducting FQT. The developer will define a preliminary set of engineering requirements for each computer software configuration item (CSCI). As part of FQT, the developer will define a preliminary set of qualification requirements for each CSCI. These requirements, to be documented in the preliminary Software Requirements Specification (SRS) for each CSCI, are to be consistent with the qualification requirements defined in the system specification. The developer will identify and describe the test cases for each FQT in the software test description (STD) for each CSCI.

b. FQT will consist of unit, component and configuration item testing. Unit testing ensures the component algorithms and logic, to include Y2K compliance, employed by each unit are correct and that the unit satisfies its

specified requirement. Component testing ensures that the component algorithms and logic are correct, that they satisfy the specified requirements and that the subordinate components and units are integrated properly. Configuration items testing ensures that the entire program operates according to design specifications.

c. Throughout the Stage 1 process the functional proponent and functional users will be involved as both observers and commentators on the test results. The schedule and location for the functional proponent and functional users participation will depend on specific segment and application development.

d. The DDA will then deliver the software to the government upon satisfactory completion of FQT in accordance with MIL-STD 498, and per guidance contained in the Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 3.0, Specification/Draft, dated 1 January, 1997. Satisfactory completion of this testing is a prerequisite for the subsequent testing stages.

(2) **Compliance, Functional, and Configuration Definition/Integration Testing.** Stage 2 includes Compliance, Functional and Configuration Definition Integration Testing. All GSPRs are re-tested and validated as corrected or returned to the developer for correction. All segments are verified as complete and integrated into the GCCS version. Segment installation and integration instructions and system documentation are developed and verified. Functional users will participate in or witness testing of selected GCCS V3.0 capabilities in this stage. JITC will provide oversight and guidance to Joint Interoperability Engineering Organization (JIEO) to ensure that the exit criteria for Stage 2 has been met and software metrics are captured to effectively measure Stage 2 events.

a. Compliance Testing. Segments will be delivered to the GCCS program in accordance with the GCCS Configuration Management (CM) Delivery Letter. All segments will have been functionally proven/accepted by functional proponent prior to delivery to the GCCS program. All segments to include selected COTS and Government Off The Shelf (GOTS) software components proposed for integration into the core system will be compliance tested in accordance with the DII I&RTS (low level integration with COE & associated segment) to ensure that they have been integrated with the COE and that they work with associated segments in the COE and do not damage the environment. A compliance checklist extracted from the I&RTS is utilized to validate each segment.

b. Individual Segment Functional Testing. Random sampling of the individual segment functionality using developer provided test plans will be tested. In the absence of test plans, individual segment test checklists and procedures will be developed. The functional testing also includes

validation of the system build/upgrade procedures (Solaris, HP, and NT), validation of segment installation instructions (Solaris, HP, and NT), validation of problem reports/fixes, and backward compatibility between versions.

c. **Configuration Definition/Integration Testing.** Configuration Definition testing involves integrating CSCIs with interfacing hardware configuration items (HWCIs) and CSCIs, evaluating the resulting groupings to determine whether they work together as intended, and continuing this process until all CSCIs and HWCIs in the system are integrated and evaluated. It is designed to verify the proper integration of the configuration items with each other, and with the system environment. This process is designed to test the critical functionality of a critical mass of applications after integration with a GCCS version. This testing includes validating interfaces with Service and CINC applications migrating to or coexisting with GCCS. The testing will be performed in a lab environment at the OSF. Multiple GCCS nodes (a node includes a database server, application servers, and client workstations) will be utilized during this stage to validate database synchronization and system interfaces across a simulated wide area network. This testing also includes developing detailed system documentation as described in paragraph 2.1.1b(5).

(3) **MDT/System Testing.** Stage III consists of conducting application and system testing, at selected MDT sites, to verify integration and functionality, lead to a recommendation on acceptance, and prepare for an Operational Test Readiness Review (OTRR) with full user involvement. Users will evaluate if the functional and technical user requirements are met. Interfaces with feeder systems, when made available, will be evaluated. Priority 1 & 2 GSPR fixes, that were not validated in previous stages, will be validated. Some GCCS application functions will be selected for inclusion into the Performance Characterization effort. The Performance Characterization effort will test, track, and record application response times during testing. Performance Characterization data can be later used by operational sites as a rough yardstick for planning and comparison purposes of their GCCS suites. JITC, working with user Subject Matter Experts (SMEs), will ensure that the exit criteria for Stage III have been met and that the results provide enough data to facilitate an OTRR decision.

- a. During this stage, JITC will work with users and verify the installation procedures and software load programs for each available platform type. The MDT sites will use the procedures in the GCCS Version 3.0 release notes to produce the system. The MDT sites are JITC lab at Ft. Huachuca, JITC lab at JDEF, and designated operational sites. The certified/accredited security features and procedures will be in place. Representative System Administrator, Network Manager, Security Manager, and Database Managers will validate their procedures. The JITC will document any abnormalities. DISA will either fix the problem or revise the installation procedures to document the error/workaround. The testing will validate that the mission specific software performs as designed under realistic operational constraints. The test will exercise the system in a multi-node environment. This will serve to validate

the Wide Area Network (WAN) configuration. Using the DISA provided user level documentation, the functional users and technical support staff will, with the aid of the JITC test team, evaluate the systems capabilities as defined in the RID and EPIP.

- b. Service feeder systems, whenever available at the MDT sites, will be included in testing during this stage. Their interoperability with GCCS will be evaluated. OT&E team members will be involved at this stage as independent observers for data collection purposes in preparation for subsequent OT activities. Service feeder systems not available during this stage, will be evaluated for interoperability with GCCS during the OT&E.

- c. Results.

- (1) Quick look. Shortly after completion of this stage, a “Quick Look” report will be generated to summarize the results. This report will include the initial analysis of the performance characterization of GCCS functionalities. It will be provided to the developer, functional user, and operational tester to be used in support of the OTRR

- (2) Formal report. The formal MDT Stage III report detailing all the results will be published within a few weeks of this stage’s completion. It will be published IAW DTSE&E Policy Guidance for Software-Intensive Systems in Support of Recommendations from the GAO, 23 May 94 and OSD, Operational Test and Evaluation Memorandum, Subject: Software Maturity Criteria for Dedicated Operational Test and Evaluation of Software-Intensive Systems, 31 May 94..

**Table III-2. MDT PRODUCTS**

<b>STAGE 1 Application &amp; Segment Testing</b>		<b>STAGE 2 Compliance and Integration Testing</b>		<b>STAGE 3 MDT/System Testing</b>	
<b>JITC</b>	<b>OTHER AGENCY</b>	<b>JITC</b>	<b>OTHER AGENCY</b>	<b>JITC</b>	<b>OTHER AGENCY</b>
Requirements Baseline	Delivery Letter	Segment & Compliance Validation Report	SW Version Description	Formal Test Scenario (including test events)	Final Accreditation
Metric Standards	List COTS License	GSPR Validation Report (Re-Test)	IATO or Final		
Detailed Test Plan*	Version Description Document	COE Compliance Validation Report	STE	Performance Characterization	
Software Test Plan*	System Requirements Specification	Functional Test Report	Interface Design Document	Anomaly Report	
Software Test Description	Database Design Document	Configuration Test Report		Quick Look Report	
User Validation Report	Installation Procedures	Installation Procedures*		- Emerging Results	
System Status Report	Software Test Plan	Performance Metrics*		Formal MDT&E Report	
	Software Test Description	SOP for Exercising Segments		System Status Report	
	Operators Manual	System Status Report			
	System Administrators Manual				
	System Users Manual				
	Segment Description (Output)				
	Segment Abstract				
	Release Restriction Instructions				
	Segment or Patch List				
	Performance Metrics				
	Security Plan				
	Collected Metrics				
	Interface Design Document for Various Interfaces				
* Input/comments only. Note: Some reports may be combined					

c. Test Facilities. Test facilities available to be used to test the GCCS include the JITC test bed at Fort Huachuca, AZ; the Joint Demonstration and Evaluation Facility (JDEF) in Arlington, VA; the Operational Support Facility (OSF) in Sterling, VA; and designated operational sites. Each of these facilities will include GCCS operating platforms, software, and communications equipment necessary to operate as an operational GCCS site and will have remote access to the various CINC and Component GCCS sites worldwide. Thus, each facility will be able to support test case development, system performance analysis, joint exercises, GCCS user workshops, and other system demonstrations. These facilities provide an excellent capability to balance testing done in laboratory and operational environments

### **3.2 Developmental Test And Evaluation to Date**

GCCS Versions 1.1, 2.0, 2.1, and 2.2 have been installed along with the GCCS hardware environment consisting of open system servers, workstations, and COTS capabilities.

a. Version 1.1 included the initial release of the Common Operating Environment (COE) upon which future development efforts were based.

b. Version 2.0 included additional Service software applications and COTS integrated with the COE including UB, APPLIX, JMCIS, CHATTER, GSORTS, LOGSAFE, JFAST, UCCS, DART, IMS/RFM, S&M, and JDISS. Unit, component, and configuration item tests were done by the developing agency. Compliance, functional, installation and configuration definition tests were done by JIEO.

c. Version 2.1 included several new and updated segments to include the following: AIRFIELDS, AMHS, APPLIX, CCAPPS, Executive Manager, FTP, COE, GSORTS, GTN, IMS/RFM, RDA, JMCIS, JEPES, JOPEs Core Database, Scheduling and Movement (S&M), RFA, EVAC, JOPEs AHQ and TARGET. The complete list of segments included in GCCS 2.1 is documented in the GCCS 2.1 Version Description Document. A GCCS 2.1 multi-node SIPRNET test among the DISA/OSF, JITC and JDEF was completed in September, 1995 as was GCCS 2.1 JOPEs developmental testing. The results of the functional testing of GCCS 2.1 and SIPRNET multi-node tests documented software deficiencies that were being corrected as part of 2.1 updates.

d. Version 2.2 included fixes to GSPRs, several updated segments, a patch roll up AMHS, CCAPS, DART, IMS/RFM, LOGSAFE, RDBMS, PERL, S&M, SYBASE and TCCEsI, as well as the added features of VOLUME MANAGER, NETSCAPE BROWSER 3.0, MAIL SERVICES, and EMPIRE. The complete list of segments included in GCCS 2.2 is documented in the GCCS 2.2 Version Description Document. A GCCS 2.2 multi-node SIPRNET test among the DISA/OSF, JITC and CENTCOM was completed in January, 1997. The results of the functional testing of GCCS 2.2 and SIPRNET multi-node tests documented software deficiencies that are being corrected as part of 2.2 updates.

e. The software risk, maturity and other related issues will be addressed throughout the DT/OT process terminating in the SOR decision. However, a history of the GSPRs will be available during MDT&E. The software risk management will follow the guidance provided in the following and other pertinent documents.

(1) Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Specification/Draft, Version 3.0, January 1, 1997. OPR: DISA Chief Engineer.

(2) Director, TSE&E, OUSD/A&T Memorandum, Subject: DTSE&E Policy Guidance for Software-Intensive Systems in Support of Recommendations from the GAO, 23 May 94.

(3) OUSD, Operational Test and Evaluation Memorandum, Subject: Software Maturity Criteria for Dedicated Operational Test and Evaluation of Software-Intensive Systems, 31 May 94.

**3.3 Future Modified Developmental Test and Evaluation (MDT&E).** MDT&E for GCCS version 3.0 and future versions will follow the testing outlined in the paragraphs above. Table III-3 lists the future test events. Future revisions of the TEMP will include follow-on test events.

**Table III-3. GCCS Future Developmental Test & Evaluation Events**

Software Version	Software Description	Evaluation Objective	Test Event(s)	Limitations
<b>3.0</b>	JOPES Unified Build Service Interface Tests (AFGCCS, AGCCS, MAGTFII) Automated message handling system Teleconferencing Joint mission applications Reference File Administration Other	Determine whether to field the version 3.0..  Compliance with DII COE I&RTS	(1) Unit, Component, Configuration Item Tests. (2) Database synchronization (3) Database Backup/Recovery Test. (3) Database Snapshot (4) Multi-node User Test (MUT) (5) Stress Test (6) Transition Test (7) Y2K Compliance Test	Crisis level test scenarios
<b>3.X (Tentative)</b>	Additional CINC/Service applications	Determine entry into OT&E  Compliance with DII COE I&RTS	(1) Unit, Component, Configuration Item Tests. (2) Database synchronization (3) Database Backup/Recovery Test. (3) Database Snapshot (4) Multi-node User Test (MUT) (5) Stress Test (6) Transition Test (7) Y2K Compliance Test	Crisis level test scenarios

## PART IV

### OPERATIONAL TEST AND EVALUATION OUTLINE

#### 4.1 Operational Test and Evaluation Overview

**a. Purpose.** To determine the operational effectiveness and operational suitability of GCCS V3.0 in support of a Joint Staff J-3 decision concerning declaration of V3.0 as the DoD Command and Control System of Record.

**b. Scope.** The JITC, in collaboration with the Service Operational Test Activities, will conduct the OT under operationally realistic conditions using production representative equipment suites and actual operator personnel. Test activities will occur at operational sites and at laboratory sites. Two primary measures of effectiveness (MOEs) will be evaluated:

! Primary MOE 1. Success of Mission Tasks.

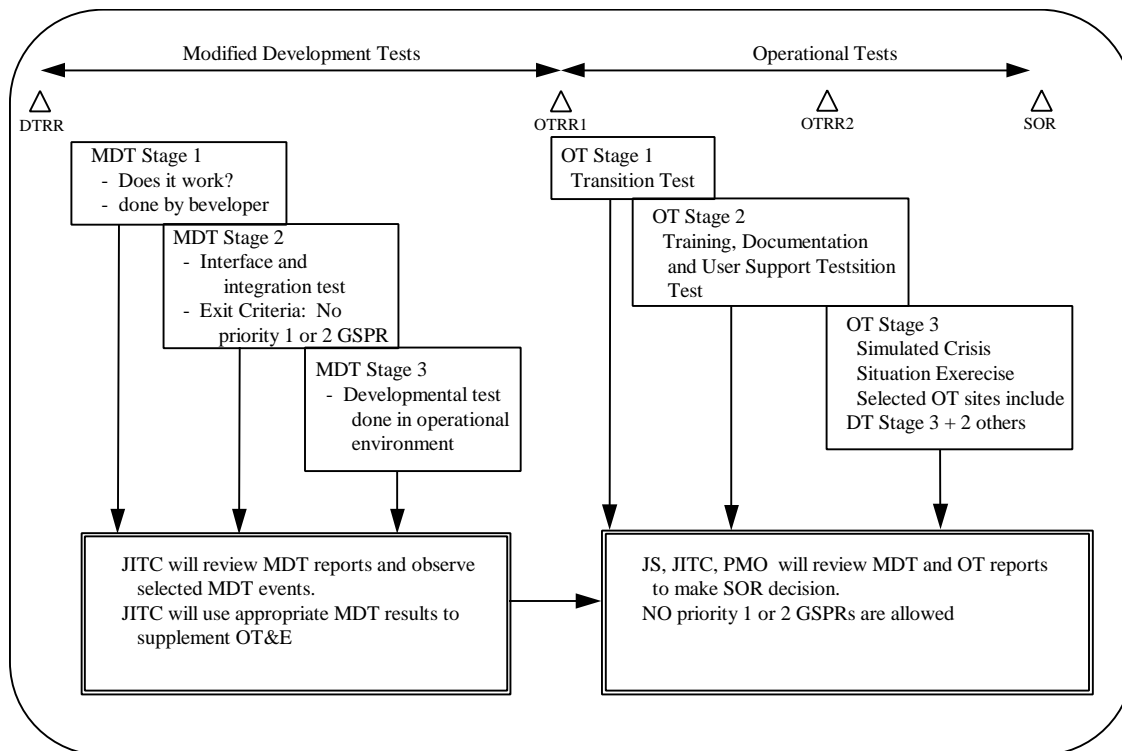
! Primary MOE 2. Success of Mission Support Tasks.

These MOE are investigative; no criteria are established for number or percent of tasks successfully completed.

Figure IV-1 illustrates the OT&E concept. OT will consist of three stages and will be supported by data from MDT. The three OT stages may overlap and are:

! **Transition Test.** This stage will occur at multiple sites. The focus will be to evaluate the success of Mission Support Tasks as performed by system administrators, data base administrators, system security administrators, and other support and administrative personnel. This stage will also document the compatibility of GCCS v2.2 clients operating with GCCS v3.0 servers.

! **Training, Documentation, and User Support Test.** This stage does not include test activities. It includes evaluation only. It is designed primarily to determine the degree to which deficiencies previously observed in training, documentation, and user support (for example, help desk support) have been corrected. Functional user support activities will be evaluated as they currently exist for GCCS Version 2.2. Functional user and technical training programs established for V3.0 at JOPEs Training Office (JTO) and AETC will be evaluated. V3.0 functional user documentation will be evaluated. System technical documentation provided by DISA to C/S/A system administrators (as described in paragraph 2.1.1b(5)) will be evaluated, to assess its completeness, accuracy, and timeliness, and its ability to support the Transition Test. A portion of the evaluation of this system documentation must take place prior to the Transition Test, in order for the Transition Test to proceed



**Figure IV-1. GCCS Version 3.0 OT&E Strategy**

- ! **Simulated Crisis Situation Test.** The user community (Joint Staff and CINCs) will designate participating operational sites. The site designated as the supported CINC will select an OPLAN to use for test purposes. Actual users at operational sites will use GCCS to support crisis action planning and execution. It is important to select a robust plan that will exercise a broad representative sample of GCCS functions as identified in the RID (for example, JOPES, COP, intelligence, SORTS, and miscellaneous functions).

The system configuration will be established at the start of the Stage III test and will not be changed during this stage except as determined necessary by the JITC to support test operations. It may be necessary (and desirable) to make configuration changes after the transition test and before the simulated crisis situation test. The GCCS PMO will coordinate with the JITC prior to making such changes. The system configuration will be re-established at the start of the simulated crisis situation test and will not be changed during this stage except as determined necessary by the JITC to support test operations.

**c. Joint Interoperability.** The Joint Interoperability Test Command (JITC) is required by DODI 4630.8 and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01A to certify C4I systems for interoperability with Joint Systems with which they have a requirement to exchange information. At the end of Modified Developmental Testing (MDT), JITC must certify conformance of standards and at the end of Operational Test and Evaluation (OT&E), JITC must certify interoperability. JITC will review GCCS test plans and procedures to ensure that the data

to be collected meet the JITC requirements. JITC will monitor interoperability requirements during various GCCS tests and use the data to evaluate system interoperability.

JITC is required to certify and report Y2K compliance and status in the OT&E report IAW DOT&E letter, 25 Apr 1997

#### **4.2 Critical Operational Issues.**

System requirements for GCCS Version 3.0, as established in the RID, lead to these five critical operational issues:

**Operational effectiveness.** Primary MOE 1, Success of Mission Tasks, is the principal test measure for operational effectiveness.

**COI 1. Mission performance.** Does the GCCS support warfighters in accomplishing deliberate and crisis action planning and execution in an operational environment?

This COI will be evaluated on the basis of Mission Task success in the context of an operationally realistic simulated crisis situation test.

**COI 2. Interoperability.** Does the GCCS support the effective exchange of information required to plan and execute missions? The areas that will be assessed to answer this COI are:

1. The interoperability of GCCS with other DoD systems.
2. The capability provided to the planner to use information provided by external organizations and to produce information used by external organizations.
3. The exchange and processing of data related transaction is not corrupted/compromised after Dec 31, 1999.

**COI 3. Security.** Does the GCCS architecture provide the necessary security precautions to protect the military operations and national objectives supported by the GCCS?

**Operational suitability.** Primary MOE 2, Success of Mission Support Tasks, is the principal test measure for operational suitability.

**COI 4. Mission Support.** Can GCCS be installed, configured, and maintained effectively at operational sites? This COI will be evaluated on the basis of Mission Support Task success in the context of the Mission Support Test.

**COI 5. Supportability.** Is the GCCS capable of supporting sustained operations in an operational environment?

- a. **User support.** Is the GCCS help desk and supporting infrastructure capable of supporting GCCS users in an operational environment?
- b. **Training.** Does the training program provide GCCS functional users and technical support staff (system and database administrators, etc.) the skills required to perform their operational tasks on the GCCS?
- c. **Documentation.** Does the user-level documentation provide GCCS users adequate and complete information on how to accomplish their operational tasks on the GCCS?
- d. **Accessibility, Consistency, and Dependability (ACD).** Does GCCS V3.0 provide a level of accessibility, dependability and consistency to allow operational users to complete the mission?

GCCS is a highly distributed, client-server, multiprocessor environment in which the traditional measures of reliability, availability, and maintainability (RAM), are impractical to define. It is also a GOTS/COTS integrated product which has already been deployed operationally, so RAM testing will not be performed in the traditional manner. Instead, this program will establish a new paradigm which defines and measures accessibility, dependability, and consistency.

1. Definitions of the new measures:

a. Accessibility is the ability of users to logon and begin executing those processes in support of their mission operations at any point in time.

b. Dependability is the ability of the system to complete user initiated processes to the user's satisfaction. Note that this measure may be split into two aspects 1) the ability to eventually complete the process, and 2) the frequency of interruptions due to hung processes, restarts, and other processing difficulties.

c. Consistency is ability of the system to provide the same results to a given process independent of where it is initiated and, if the underlying data has not changed, independent of when it is initiated.

2. Accessibility and dependability testing will evaluate both the technical and procedural issues. Accessibility and dependability testing will involve three levels: User level; LAN level; WAN level.

a. The User level will address the frequency and duration of delays, outages, blank screens, and "lock out". Outages and delays will be further defined in order to provide precise testing criteria.

b. The LAN level will address service at the site. This includes accessibility and dependability for the local application servers, local database, and intra-LAN users.

c. The WAN level will address ability to get service from and to the SIPRNET to include accessibility and dependability for external databases, users at other sites, COP feeds, and Internet.

3. Measures of evaluation and measures of performance will be developed in the test plans. GCCS V3.0 is being fielded incrementally, and ACD will be evaluated in these new measures in increments as well.

a. During the GCCS version 3.0 OT&E, accessibility will be addressed fully. Dependability will be evaluated if the user reporting, system administration tools, and technical monitoring tools are able to provide valid and timely results. Consistency will be evaluated by exception only.

b. Dependability and consistency, will be tested during the modified DT, limited functional test after the transition test, and during subsequent OT stage 2 increments. Dependability will be measured by monitoring task completion rates and process restoral rates. Consistency will involve evaluating whether the results are always the same for parallel sessions and for repeated trials on an unaltered database.

#### **4.3 Operational Test and Evaluation to Date**

No OT&E has been performed for GCCS Version 3.0. However, the JITC, Service Operational Test Agencies (OTA), and several user groups conducted OT&E of V2.1 during April-August 1996. As a result, the Joint Staff declared V2.1 the DoD C2 System of Record and shut down the legacy WWMCCS. The JITC, CENTCOM, and COMOPTEVFOR conducted an operational assessment of V2.2 in December 1996. As a result, V2.2 was distributed to the field as a replacement for V2.1.

It is currently planned that V3.0 will add some new functionality over that in V2.2. The primary objectives of V3.0 are:

- ! Replace the GCCS COE with the DII COE
- ! Upgrade versions of the GCCS workstation operating systems
- ! Upgrade the version of the Oracle Relational Database Management System (RDBMS)
- ! Replace the current government-developed desktop with a commercial desktop.
- ! Provide some high priority GSPR fixes
- ! Correct security deficiencies
- ! Provide some new functionality in the areas of:
  - JAVA based Airfields
  - Tactical METOC capability
  - JTAV client
  - JPAV client
  - TBMD Segment
  - MIG/MIGDB access and display (Renamed to TC4I)
  - Imagery Product Library (IPL) access and display
  - TRE interface to support TBMD

Production quality receive-only interfaces for:  
TIBS, TADIL B, PLRS/EPLRS

Thus it is necessary to test the existing and new functionality in the context of the new COE, operating system, RDBMS, and desktop.

Testing of V3.0 is further required because OT of V2.1 and V2.2 was limited by these factors:

- ! **Questionnaire responses of limited value in assessing GCCS V2.1.** In testing V2.1, 28 of 48 test measures were based on user assessments; the primary data source for these assessments was intended to be user questionnaires. However, because of limitations in the collection of questionnaire responses, the JITC assigned a low weight to the responses and instead relied on other sources for the user assessments.
- ! **Functional checkout of GCCS V2.2 not operationally realistic.** The OA of V2.2 was based on Beta testing, which consisted primarily of functionality checks performed without a realistic operational scenario.
- ! **Validation of Year 2000 compliance was not accomplished** The Y2K requirements were not established at the time GCCS v2.1 underwent operational testing.

#### **4.4 Future Operational Test and Evaluation.**

Testing of V3.0 will overcome the shortcomings noted above for testing of V2.1 and V2.2.

**4.4.1 MDT Support of OT.** The JITC will review MDT test results, which will be provided by the PMO, and may observe selected MDT events. JITC will use applicable MDT results to support the OT&E. The JITC will be leading the MDT Stage III and beta testing as a part of OT Readiness Review.

**4.4.2 Transition test.** The test will be task driven, and the evaluation will focus on success of Mission Support Tasks accomplished by test players.

##### **a. Measuring Mission Support Task Success**

A list of potential Mission Support Tasks is at PART IV Appendix, Table 9. The functional and technical user community will determine the final task list. A Mission Support Task is an action that must be performed by a GCCS system administrator, database administrator, security manager, or other support person to install, set-up, configure, or otherwise prepare the system for operational use; it should take about one to four hours to complete.

The functional and technical user community will establish the criterion for success of each task based on timeliness, ease of performance and adequacy of training and documentation to perform the task. The following is a proposed scale:

Unsuccessful. The task could not be performed by the assigned personnel.

Marginally successful. Task performed in a reasonable time, but with workarounds. Documentation lacks sufficient details. Task not fully covered in applicable training.

Fully successful. Task easily performed in a timely manner. Task fully covered in applicable training. Documentation accurate, complete, and readily available.

The functional and technical user community may categorize the tasks according to their importance to overall mission accomplishment. If so, the JITC will consider the user priorities in the evaluation.

The functional and technical user community will provide subject matter experts (SMEs) to evaluate success of Mission Support Tasks accomplished by test players. The JITC will investigate causality for any non-successful Mission Support Tasks.

**b. Test sites.** Operational Test and Evaluation sites will include operational sites and lab sites. To preclude disruption of operational missions, operational sites will use spare (not operational) equipment suites.

#### **4.4.3 Training, Documentation, and User Support Test.**

This stage of OT focuses on COI 5 Supportability (except ACD). It may be completed before the other two OT stages. It will consist of three separate evaluations, as described below.

**Training evaluation.** JITC will evaluate the following training courses conducted by the JTO and AETC:

##### Training to support Mission Support Tasks

- Database administrator training
- System administrator training (HP/UX, Solaris, NT)
- Security manager training
- Network manager training
- AMHS administrator training
- NET-New Equipment Training, to include loading, debugging, and correcting V 3.0 installation procedures

##### Training to support Mission Tasks

- GCCS User Introduction
- GCCS Action and Planning Staff Orientation
- Training to support user requirements for:
  - Resource and unit monitoring (GSORTS and RFA)
  - Conventional Planning and Execution (JOPES and JOPES-related)
  - Other Joint requirements (Airfields, EVAC, teleconferencing applications, TELNET and file transfer)
- Interoperability (AMHS)

Common Operational Picture

Air Tasking Order  
Access to intelligence data  
Support applications such as Applix

The evaluation will focus on the effectiveness of the training to prepare the functional user to perform the mission using GCCS V3.0 and the technical support staff to efficiently perform the transition from 2.2 to 3.0, and the follow-on support of 3.0. A principal input to the evaluation will be interviews with personnel at selected sites to determine the user's perspective of training effectiveness. The JITC will attend selected courses to support the evaluation of training.

**Documentation evaluation.** This evaluation will commence as documentation becomes available for review in draft form. The intent is to influence final documentation. JITC will review and evaluate the following user documentation:

Operator's manual  
Installation procedures  
System administrator's manual  
Software user's manual

Other user documentation such as application-specific user manuals .

Detailed system documentation:

- a. Contents of the new load: file laydown, files and directories created and written to by the load process, and files overwritten.
- b. Server configuration information: file system size estimates/minimums; expected NFS mounted file systems; extent of TFM compliance. DISA must clearly identify any files, structures, etc. that must be set or re-set at the site.
- c. Individual application details: application name; developer; short functional description; software run requirements; directories (what files are being placed in which directories); Lists of software on clients and on servers; initiating sequence; sequence of launch events; icon bitmap files; names of source files; what are the user-configurable files for the application; What system-level variables are being set by each application; Does the application rely on remote shelling for execution; Does the application reference alias host names; Dependency chart between applications, i.e., How application affects or uses information from other applications (tables being updated, files being replaced, CPU requirements/effect of a CPU-bound process on other applications and on itself when it has less than its optimum CPU share)
- d. List of system and application/segment default settings: when a particular application is installed, does the installation overwrite the current account configurations? Some applications have user- or SA-configurable flat files. If default settings are documented, SA's will be able to re-configure for the new version.
- e. Account migration process for 2.2 user accounts, authorizations, privileges, and data. This account and data migration will be the driving factor in the resulting downtime from the users' perspective. The description should include the following areas:

- (1) Pseudo-code demonstrating how the migration process from v. 2.2 to 3.0 handles the range of account folders (personal and shared folder types: project, position, directorate, division, branch, section, cell), all of which are under the shared global folder directory.
- (2) Advance notification and description of the amount of manual labor in account and data migration.
- (f) Description of the new login access mechanism and account management mechanism.
- (g) Description of Installer.
- (h) Database Entity Relationship Model/Diagram and Data Dictionary

In addition, JITC will interview personnel at selected sites. The evaluation will focus on the following factors:

- Availability of documentation to functional and users technical support staff at operational sites, to include ease of access, downloading, printing, and declassification.
- Accuracy
- Usefulness
- Currency with respect to V3.0 software
- Completeness.

**User support evaluation for Transition from 2.2 to 3.0 (Part One).** For part one of the User Support evaluation, JITC will review and evaluate DISA procedures, technical training, and system documentation for system administrator support, as described in paragraphs 2.1.1.b.(5) and 4.4.3 (*documentation evaluation*) above. This review will concentrate on evaluating the completeness, accuracy, and timeliness of the training/documentation specific to the transition from 2.2 to 3.0.

**User support evaluation for post-SOR (Part Two).** For part two of the user support evaluation, JITC will review and evaluate existing procedures for functional and technical user support; that is, the procedures in place for V2.2. This evaluation applies to V3.0 because the user support concept does not change between V2.2 and V3.0. This will include (but will not be limited to) the Help Desk. This review will concentrate on the support to be provided after 3.0 is the system of record and all servers and clients have been transitioned. This review will include interviews with personnel at selected operational sites. The evaluation will focus on:

- Differences between user support for v2.2 and v3.0
- In OT stage 3, key elements of support that were identified during OT stage 2
- Effectiveness of user support in providing technical assistance to the user
- Accuracy of responses
- Timeliness of responses
- Completeness of responses
- Usefulness of responses to the user in supporting the user mission.

#### **4.4.4 Simulated Crisis Situation Exercise.**

The exercise will include a planning phase and an execution phase. Staff elements from the

supported and supporting CINCs, appropriate components, a simulated JTF, and the NCA will participate. The test will be task driven, and the evaluation will focus on success of Mission Tasks accomplished by test players.

**a. Measuring Mission Task Success.**

A list of potential Mission Tasks is at PART IV Appendix, Tables 2 through 8. The user community will determine the final task list. A Mission Task is a staff action that requires GCCS support to accomplish and that has a defined product; it should take about one to four hours to complete.

The functional user community will establish the criterion for success of each task based on the timeliness, accuracy, completeness, and usefulness of the task product. The following is a proposed scale:

Unsuccessful. No product or product cannot be used by the intended recipient for the intended purpose or it is too late or inaccurate to support the mission.

Marginally successful. Product requires workarounds to produce, or the intended recipient must use workarounds to use the product for mission accomplishment, but the output is reduced within an acceptable time and is accurate.

Fully successful. Product is sufficiently timely, accurate, complete, and useful that it fully supports mission accomplishment by the intended recipient.

Highly successful. Product exceeds requirements for timeliness, accuracy, completeness, or usefulness.

The user community may categorize the tasks according to their importance to overall mission accomplishment. If so, JITC will consider the user priorities in the evaluation.

The user community will provide subject matter experts (SMEs) to evaluate success of mission tasks accomplished by test players. The JITC will investigate causality for any non-successful Mission Tasks.

**b. Test sites.** Test sites will include operational sites and lab sites. To preclude disruption of operational missions, operational sites will use spare (not operational) equipment suites, as available. The sites will be configured to represent the NCA, supported CINC and components, supporting CINCs, JTF and components, and other players as necessary.

## PART IV APPENDIX - MISSION TASKS AND MISSION SUPPORT TASKS

The following information has been extracted from the GCCS User Characterization Profile and other sources to produce a partial listing of possible mission/mission support tasks for testing GCCS Version 3.0.

**Crisis Action Procedures.** CAP provides a framework for describing the unfolding of a crisis requiring a military response. Table 1 lists the six CAP phases.

**Table 1. CAP Phases**

Phase	Title
I	Situation Development
II	Crisis Assessment
III	Course of Action Development
IV	Course of Action Selection
V	Execution Planning
VI	Execution (Includes redeployment)

Each phase is punctuated by one or more scenario events. The scenario event usually triggers a response from one or more of the Joint Planning and Execution Community (JPEC) players in the crisis. Many responses consist of an activity supported by the GCCS. The trace from a scenario event to the GCCS activity performed by specific JPEC member(s) is contained in the CAP Matrix that follows.

**Participant.** The scenario event triggers a response/action at certain levels in the JPEC. The actions contained in the matrix are limited to those participants with the most GCCS play. The participants listed in the matrix are:

- CJCS** - Chairman of the Joint Chiefs of Staff
- SPD** - Supported Commander
- SPG** - Supporting Commander
- USTC** - United States Transportation Command
- SVC** - Services

**Tasking arrangement.** Tables 2 through 7 contain the mission tasks for each respective phase. Table 8 contains additional mission tasks which were not specified in the GCCS User Characterization Profile, but each user should integrate these tasks into table 2 through 7 where most appropriate for their activity. In addition, each user should test desktop functions and other supporting applications within appropriate mission task areas.

Table 9 contains other Mission Support Tasks for Systems Administrators, Security Administrators, Database Administrators, JOPES Functional Database Managers, and JOPES Technical Database Managers.

**Table 2. Mission Tasks, Crisis Action Planning Matrix, Phase I**

<b><i>Phase I - Situation Development</i></b> Phase I begins with an event having possible national security implications and ends when the CINC submits his assessment of the situation to the National Command Authority (NCA) and the Chairman of the Joint Chiefs of Staff.			
<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
CJCS	Monitor the situation and evaluate reports from all sources; Request an assessment report from the supported commander	Generate a GENSER message to SPD	Message to SPD
SPD	Review message	Provide a CINC's assessment report	OPREP-3 message

**Table 3. Mission Tasks, Crisis Action Planning Matrix, Phase II**

<b>Phase II - Crisis Assessment</b> Phase II begins with a report from the supported commander and ends with a decision by the NCA to return to the pre-crisis situation, with options developed for possible consideration and possible use.			
PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT
ALL	Anticipation of action	Review OPLANs and CONPLANs for applicability	List of available/applicable plans
ALL	Anticipation of action	Review force readiness	Unit readiness reports
CJCS	Request SPD take action	Request SPD establish a crisis Newsgroups	Message to SPD
SPD	Respond to message	Implement the crisis Newsgroups	Newsgroups established; message to participants to join
ALL	Respond to message	Subscribe to Newsgroups	Newsgroups actions
CJCS	Require USTC review strategic lift asset employment availability	Generate a Newsgroups message to USTC	Newsgroups message
USTC	Review the status of strategic lift assets	Review lift asset availability; Review lift asset status	Lift Asset Reports
USTC & SPD	Determine amount of lift available for operation	Publish daily capability of lift assets; update transportation models with asset capabilities	Updated transportation Models Newsgroup message Updated TPFDD LOI posted on home page

**Table 4. Mission Tasks, Crisis Action Planning Matrix, Phase III**

<p><b><i>Phase III - Course of Action Development</i></b>            Phase III begins with a decision to develop possible military Courses of Action (COAs), normally transmitted by a CJCS Warning Order. COAs are presented to the NCA.</p>			
<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
CJCS	Establish command relationships; State mission, objectives, and known constraints; Direct the development of COAs	Publish Warning Order	Warning Order message published
ALL except CJCS	Respond to Warning Order; Initiate development of possible COAs using GCCS	Review existing OPLANs/ TPFDDs	Existing files access
ALL	Update an existing OPLAN	Refine existing supported/supporting OPLANs/TPFDDs	Modified OPLAN/TPFDD
SPD	Initiate/direct development of COAs/TPFDDs using GCCS; Publish CINC Annex to standard TPFDD LOI	Develop new COAs/TPFDDs using GCCS	Newly initiated plan Newsgroup message Updated TPFDD LOI posted to home page
ALL except CJCS	Receive new TPFDD	Review and modify new TPFDD	Develop new COAs/TPFDD using GCCS

**Table 4. Mission Tasks, Crisis Action Planning Matrix, Phase III (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
SPD	Prepare new TPFDD for evaluation	Generate sustainment records for the new TPFDD	TPFDD file processing
SPD	Request evaluation of proposed COAs	Publish an Evaluation Request; Evaluate availability, combat readiness and suitability of forces; Evaluate availability of sustainment; Evaluate database completeness	Newsgroups Evaluation Request
ALL except SPD and CJCS	Receive and review Evaluation Request		
SPD	Fatal Error Free TPFDD required for transportation analysis	Produce a logical TPFDD	Logical Errors Report; TCC Pre-edit Report TPFDD ready for transportation analysis
SPD	Request Deployment Estimate by USTC	Request USTC develop a preliminary Deployment Estimate	Newsgroups request for Deployment Estimate

**Table 4. Mission Tasks, Crisis Action Planning Matrix, Phase III (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
USTC	Review the request for a Deployment Estimate	USTC conduct Deployment estimates on each viable COA/TPFDD	Land summary and associated graphs and reports; Sea summary and associated graphs and reports; Air summary and associated graphs and reports; Airlift summary profile; Sealift summary profile; Lateness by supply class reports; Force Module Closure Profiles
		Prepare and submit Deployment Estimate Response message	Deployment Estimate Response message
SPG SPD Components	Preparation and submission of Evaluation Response to the SPD Review of Deployment Estimate Response	Prepare an Evaluation Response message (OPREP-1)	Evaluation Response message
SPD	Preparation and submission of Commander's Estimate; Recommendation of a COA; Review of Evaluation Response	Prepare and submit the Commander's Estimate	Commander's Estimate
ALL	Review of Commander's Estimate		

**Table 5. Mission Tasks, Crisis Action Planning Matrix, Phase IV**

<b><i>Phase IV - Course of Action Selection</i></b> Phase IV begins when COAs are presented to the NCA and ends when a COA is selected. The primary activity in this phase of crisis planning is the selection of a COA by the Chairman of the Joint Chiefs of Staff and NCA. All other members of the JPEC continue their activities as described in Phase III.			
<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
CJCS	Review and Evaluate COAs presented in the Commander's Estimate; Alert Order is published directing execution planning activities commence for Selected COA	Alert Order published directing execution planning activities commence for Selected COA	Alert Order
ALL	Receive and review Alert Order		
SPD	Update TPFDD Letter of Instruction (LOI)	Update the published TPFDD LOI that provides procedures for the deployment, replacement, and redeployment of the forces in support of Selected COA	TPFDD LOI

**Table 6. Mission Tasks, Crisis Action Planning Matrix, Phase V**

<b>Phase V - Execution Planning</b> Phase V begins when a Planning or an Alert Order is received and ends when an executable OPORD is developed and approved for execution. Based on receipt of the Alert Order, activities commence for further selected COA refinement and preliminary scheduling activities.			
PARTICIPANT	BACKGROUND ACTION	MISSION TASK	OUTPUT/PRODUCT
<b>NOTE:</b> The following incremental cycle includes: validation of movement requirements, scheduling of organic and strategic lift, the allocation of requirements to carriers, the reporting of actual carrier movements, and the manifesting of requirements to carriers. Any carrier itinerary diversions will continue until the deployment is complete or the crisis subsides (combined Phases V and VI).			
SPD SPG USTC	Review the TPFDD LOI	Confirm, adjust and source COA force requirements.	Adjusted TPFDD
SPG SPD	TPFDD adjusted to LOI	Schedule/allocate movements for the first increment of deployment	Scheduled TPFDD
SPG	TPFDD scheduled	Identify force. Complete SPG validation of first deployment increment shortfalls	Shortfalls listings
SPD	Review SPG force and sustainment shortfall messages	Validate the first deployment increment (first 7 days of airlift and first 30 days of sealift)	Transportation Pre-edit Report; Validated first deployment increment
SPD	Validated first deployment increment	Notify the JPEC when the first deployment increment is validated	Validation message

**Table 6. Mission Tasks, Crisis Action Planning Matrix, Phase V (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
ALL	Receive and review Validation message		
USTC (AMC)	Validated increments will be scheduled	Develop and enter Common-User Air Movement Schedules (7 days)	7 days of air schedules
USTC (MTMC) (MSC)	Validated increments will be scheduled	Develop and enter Common-User Surface Lift schedules (30 days)	30 days of surface schedules
SPG	Validated increments will be scheduled	Develop and enter organic carrier schedules	Organic Carrier Schedules
SPD	The SPD converts the COA into an OPORD	Convert the COA and publish an OPORD	Newsgroups OPORD
ALL	Receive and review OPORD		

**Table 7. Mission Tasks, Crisis Action Planning Matrix, Phase VI**

<b>Phase VI - Execution</b> Phase VI begins with the decision to execute an Operation Order (OPORD), normally transmitted by a CJCS Execute Order, and continues until the mission is completed satisfactorily.			
<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT</b>
CJCS	An Execute Order is published and issued directing the supported commander to execute his OPORD; The order directs the deployment/ employment of forces in selected COA	Issue Execute Order	Execute Order
ALL	Direct mobilization activities; Coordinate with personnel centers and logistic agencies; Identify and confirm sustainment requisitions	Monitor the initial deployment of forces; Review deployment status of Movement Requirements	Execute Order
USTC (AMC)		Report Strategic Airlift Arrival and Departures for the first increment of movement (first 7 days)	Airlift movement
USTC (MTMC) (MSC)		Report Common-User Surface Lift Arrival and Departures for the first increment of movement (first 30 days)	Surface movement
SPG	Actual arrivals/departures will be reported	Report arrivals and departures of non-strategic carriers	Non-strategic movement
<b>NOTE:</b> The above incremental cycle includes: validation of movement requirements, scheduling of organic and strategic lift, the allocation of carriers, the reporting of actual carrier movements, and the manifesting of requirements to carriers. Any carrier itinerary changes or diversions will be reported and the crisis subsides (combined Phases V and VI).			
SPD	JTF Deploys forward	Deploy GCCS forward	All required functions in austere environment

**Table 8. Additional Mission Tasks**

The following mission tasks are not included in the GCCS User Characterization Profile. They need to be inserted into the testing at app

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
EVAC User	Non-combatant personnel need to be evacuated from area of interest (AOI)	Produce and print an evacuation list for country and district of AOI	EVAC report
		Produce and print Evacuation Summary for country of AOI	EVAC summary report
Air Field Planner	Usable airfields must be made known to movement planners	Produce Airfields report for AOI	Airfields report
Common Operational Picture Users	Maps for AOI may be viewed as desired, with available tracks for all reported activity	Bring up Common Operational Picture (COP) without filters set	Display of map and tracks (may be very cluttered, depending on amount of message traffic)
		Filter out undesired tracks	Less cluttered display
	Users without COP processing can view a snapshot of COP by using ELVIS (in receive only mode)	This task will require co-located COP and non-COP workstations; Visually verify that the ELVIS picture matches the COP Picture	Active COP picture and ELVIS snapshot agree
TARGET users	Additional tools available	Exercise the TARGET functionality	

**Table 8. Additional Mission Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
UB	Air Tasking Orders can be reviewed, segmented, and segments transmitted to components as needed	Receive an ATO	ATO message
		Segment the ATO	Segments of ATO
		Transmit the ATO segments to the components they apply to	Transmitted segments received by components
COP Users	Execution of ATO results in air tracks being reported which will then appear in COP	Verify that during ATO execution, the reported air tracks correlate to the aircraft designated in the ATO	Air tracks in COP match ATO plans
Intelligence System Users	Intelligence mission requires access to resources	Provide an intelligence resources report	Resources report
		Produce a request for intelligence support	Intelligence support request
JDISS Users		Execute the intelligence mission	Intelligence gathering of imagery and sensor data
SVC	Service feeder systems must support GCCS with the new operating systems, new DII COE and new Oracle Relational Database Manager	Each service verify that the interfaces still work correctly	Services Interface Files

**Table 8. Additional Mission Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION TASK</b>	<b>OUTPUT/PRODUCT</b>
SVC/remote users	Access to documentation must be verified	Access GCCS homepage and view/download new documents	Documents on line
SVC	Maintenance of and access to Status of Resources and Training (SORTS) must be verified	Each service use access through GSORTS to verify that the service updates to SORTS is being processed and passed to GSORTS and GCCS users	GSORTS listing of selected service units

**Mission Support Tasks.** The following table presents examples of Mission Support Tasks. These tasks are performed by Security Administrators, Database Administrators, Functional Database Managers, and Track Database Managers.

**Table 9. Mission Support Tasks**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION SUPPORT TASK</b>	<b>OUTPUT/PRODUCT</b>
System Administrator (SA)	SA is responsible for installing GCCS applications on local site	Review DISA system documentation. Determine local site configuration unique settings	List of unique settings, equipment, and application install requirements
		De-install segments to be replaced	Cleaned out disk space
		Install new Solaris	New operating system
		Install new Desktop	New Desktop
		Install new RDBMS (ORACLE)	New RDBMS
	Establish/update the domain name service	Install the local domain name server	Local DNS Server
		Update DNS as needed	Updated DNS

**Table 9. Mission Support Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION SUPPORT TASK</b>	<b>OUTPUT/PRODUCT</b>
SA (continued)	Establish/update the NIS+ service	Install the local NIS+Server	Local NIS+ Server
		Create NIS+ replicas	
		Update NIS+ as needed	Updated NIS+
	Install new segments in proper order	Install new segments in proper order	New segments on system
	Provide printer support to users	Configure and manage printers for user access	Current printer file printer table
	Users require accounts and permissions to access applications	Provide accounts for database user	Database users properly established
		Provide user accounts for general access	GCCS users properly created

**Table 9. Mission Support Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION SUPPORT TASK</b>	<b>OUTPUT/PRODUCT</b>
SA (continued)	Users require accounts and permissions to access applications	Set permissions	User permissions
	Software licenses must be available and administered to provide user access to applicable applications	Acquire licenses as required; Provide user access	Usable licensed applications
	Provide for configuration management	Apply file and directory listings of all applications	File system management
	Provide Apply user support	Process Inter-relationship specifications	System Trouble shooting
	Teleconferencing capabilities must be provided to users	Install teleconferencing applications	Teleconference capabilities
	Provide mail service	Install mail service	Sendmail application
		Maintain mail admin files	Usable mail system
	Provide problem corrections	Halt system operations	All processing stops
		Reboot system in single user mode	Only root user (SA) can access system
		Reboot system in normal mode	All authorized users may log in and process applications

**Table 9. Mission Support Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION SUPPORT TASK</b>	<b>OUTPUT/PRODUCT</b>
SA (continued)	Provide system backup and recovery services	Perform routine scheduled backups	Backup files on tape or disc
		When needed, perform system recovery actions	Recovered system; ready to resume processing
	Provide GSORTS administration	Provide for GSORTS updated information	Up-to-date GSORTS files
SA and/or Sec Mgr	Provide security aspects of mission support	Setup and maintain user access accounts	User accounts files
		Setup and maintain system and user profiles	Profile tables
		Maintain roles in account groups	Account group roles
		Provide system audit capabilities	Audit logs
		Provide password administration	Password controls
DataBase Administrators (DBA)	Provide reliable database support to authorized users	Establish and maintain authorized database structure	Prescribed databases
		Perform database backup	Backup data on storage media
		Provide database recovery	Reload data from backup and process files
	Provide database maintenance capability	Apply Entity Relationship Model/ Diagram and Data Dictionary	Database Management

**Table 9. Mission Support Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION SUPPORT TASK</b>	<b>OUTPUT/PRODUCT</b>
DBA (continued)	Provide for alternate database access	Provide for user access and permissions at alternate database sites	User access and permissions files at alternate database site
		Provide alternate database access when needed	Remote database access to alternate site
JOPES Functional Database Manager (FDBM) or Track Database Manager (TDBM) as appropriate	Use the JOPES FDBM or TDBM responsibilities listing as a guide to test and evaluate mission support functions in the following areas:		
	Administrative	Permissions management	
		Teleconferencing (Newsgroups)	
		Installations	
		Backup/Recovery (JOPES Database)	
		Backup/recovery Individual TPFDDs	
		Continuity of Operations Plan (COOP)	
		Admin reporting (management)	

**Table 9. Mission Support Tasks (continued)**

<b>PARTICIPANT</b>	<b>BACKGROUND ACTION</b>	<b>MISSION SUPPORT TASK</b>	<b>OUTPUT/PRODUCT</b>
FDBM or TDBM (continued)	OPLAN Management	OPLAN initialization	
		OPLAN type/distribution/access	
		OPLAN status	
		OPLAN offload/reload	
	Network management/monitoring	OPLAN deletes	
		Set C-Day/L-Hour	
		Reset C-Day/TCC indicators	
		OPLAN synchronization	
		Reporting (user)	
		Site status	
		Transaction processing/flow (local)	
		Database maintenance and statistics	
		Transaction processing/flow (distributed network)	
		Reporting (transactions)	
	Provide JMCIS administration	Provide for JMCIS channels and JMCIS feeds	Up-to-date JMCIS files

## **PART V**

### **TEST AND EVALUATION RESOURCE SUMMARY**

#### **5.1 Test and Evaluation Resource Summary.**

a. Test Articles. GCCS test articles include all software and hardware configurations required to support GCCS Versions 3.0. Also included are software and hardware configurations of Joint/CINC/Service systems that are to interoperate with GCCS.

b. Test Sites and Instrumentation. The user community, ICW Joint Staff J-3 and the Program Management Office will select operational sites to serve as test sites. Each site will be configured in an operationally realistic manner.

c. Test Support Equipment. Hardware (e.g., personal computers) and software (e.g., data base software) are required to support any data reduction and test reporting requirements. Test support equipment should include five complete starter set configurations each with one database server, two application servers and at least two clients. Additionally, each site must have a communications router which provides access to the SIPRNET. Each test system will be installed with the GCCS release and all required COTS software components to include operating system, Relational Data Base Management System (RDBMS) and network management software.

d. Threat Systems/Simulators. None required.

e. Test Targets and Expendables. None required.

f. Operational Force Test Support. Actual users at operational sites will operate the system during the test.

g. Simulations, Models and Testbeds. Terminal emulators are required to simulate multiple users on GCCS. The various Joint/CINC/Service interfaces will be stress loaded to test GCCS' operational effectiveness.

h. Special Requirements. None.

i. Test and Evaluation Funding Requirements. Program element 50K includes an estimated 1.5 million dollars for GCCS test and evaluation in each fiscal year.

j. Manpower Personnel Training. Training to support GCCS test and evaluation includes installation training designed to train personnel to install segments and load the database prior to the beginning of the user pre-assessment. The DISA will provide training on the GCCS system administration and applications prior to the user assessment. Studies within each of the Services are currently underway to determine training requirements. Table V-2 lists test personnel requirements for the OT.

**Table V-1 Operational Test (OT) Personnel Requirements**

<b>EVENT</b>	<b>TEST PERSONNEL</b>
Normal Operations	No dedicated personnel required. Users perform day-to-day task at 37 GCCS sites.
MDT Phase 1/2 (User Involvement)	JITC/Users evaluation team: Sites, dates and numbers TBD.
MDT Phase 3 (BETA Test)	JITC/Users evaluation team: Dates and numbers TBD.
JOPEs Database Refinement Conference	JCS/J7 Test Team: (TBD) Users: Conference attendees JITC: TBD observers Components: Test personnel as coordinated
Operational Test	Selected CINC/component sites: System Administrator, users, crisis action teams per J33 LOI.* JITC: TBD data collectors OSF: TBD System Administrator, data collectors

\* Will be coordinated with J3



## APPENDIX A

### GLOSSARY

AFOTEC	Air Force Operational Test and Evaluation Command
ASDC <sup>3</sup> I	Assistant Secretary of Defense, Command, Control, Communications, and Intelligence
AHQ	Ad Hoc Query
C2	Command and Control
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4IFTW	C4I For the Warrior
CINC	Commander In Chief
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJTF	Combined Joint Task Force
COA	Course of Action
COE	Common Operating Environment
COMJTF	Commander, Joint Task force
CONOPS	Concept of Operations
COTS	Commercial Off-the-shelf
C/S/A	CINC, Service and Agency
CSCI	Computer Software Configuration Item
DDA	Designated Development Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DODIIS	DoD Intelligence Information System
DOT&E	Director, Operational Test and Evaluation
DT&E	Developmental Test and Evaluation
DTSE&E	Director, Test, Systems Engineering and Evaluation
EPIP	Evolutionary Phased Implementation Plan
FQT	Formal Qualification Testing
GCC	Global Command and Control
GCCS	Global Command and Control System
GOTS	Government Off-the-shelf
GSPR	GCCS System Problem Report
IMS/RFM	Information Management System/ Reference File Managent
IRM	Information Resource Management
JCS	Joint Chiefs of Staff
JDEF	Joint Demonstration and Evaluation Facility
JEPES	Joint Engineer Planning and Execution System
JFAST	Joint Flow and Analysis System for Transportation
JIEO	Joint Interoperability Engineering Organization
JITC	Joint Interoperability Test Command
JOPES	Joint Operations Planning and Execution System
JTF	Joint Task Force

## **APPENDIX A**

JTO	Joint Operation Planning and Execution System (JOPES) Training Office
LAN	Local Area Network
LOGSAFE	Logistics Sustainment Analysis and Feasibility Estimator
MAV	Minimum Acceptable Value
MCOTEA	Marine Corps Operational Test & Evaluation Activity
MDT&E	Modified Development Test and Evaluation
MES	Measure of Effectiveness and Suitability
METOC	Meteorology and Oceanographic
MNS	Mission Needs Statement
MUT	Multi-node User Test
NCA	National Command Authority
OPLAN	Operations Plan
OPTEC	Operation, Test, and Evaluation Command (US ARMY)
OPTEVFOR	Operational Test and Evaluation Force (US NAVY)
OSD	Office of the Secretary of Defense
OSF	Operational Support Facility
OTA	Operational Test Agency(ies)
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review
PDR	Pre-Defined Reports
PMO	Program Management Office
RDBMS	Relation Data Base Management System
RDA	Requirements Determination Analysis
RFA	Reference File Administrator
RFM	Reference File Management
RID	Requirements Implementation Document
S&M	Schedueling and Movements
SOR	System of Record
SQL	Structured Query Language
T&E	Test and Evaluation
TBD	To Be Determined
TDS	Transaction Distribution Services
TPFDD	Time Phased Force Deployment Data
Y2K	Year 2000
WAN	Wide Area Network
WWMCCS	World Wide Military Command and Control System

## **APPENDIX B**

### **SYSTEM INTERFACES**

This appendix describes the interfaces internal and external to GCCS. Since GCCS is a system of functions performed by many different applications that interact with many external systems and databases, it is necessary to clearly define the separation between internal and external interfaces. GCCS is defined to include within its boundaries those software items under the configuration management of DISA. GCCS includes all of the items that DISA owns, maintains, and updates for all GCCS sites.

#### **INTERNAL INTERFACES**

The GCCS Core database is the centerpiece of GCCS Version 2.1. and will be the first DoD CIM compliant, standardized database. Between GCCS sites, the Core databases communicate via the SIPRNET and ORACLE transactions. Within a GCCS 2.1 site, there are three ways that applications relate to the database. Some applications exclusively depend on the database for operation. Some applications require data from the Core database to be loaded into their own unique database for operation. The remaining applications do not use any data from the Core database.

#### **DATABASE DEPENDENT**

S&M, AHQ, PDR, IRM, RFA, RDA: These applications are each separate entities that do not interact directly with each other but directly access data in the Core database, update the database using SQL Plus, and create transactions which update the Core database through Transaction Distribution System (TDS). If the transactions are for networked OPLANS, the transactions will also be addressed and sent to other appropriate GCCS Core databases.

#### **REQUIRED DATABASE DATA**

TPEDIT, JEPES, JFAST, LOGSAFE: These applications do not interact. Each of these interact directly with LOGSAFE. These applications use IMS and RFM to obtain data from the Core database. IMS provides a means to move TPFDD data between the Core database and the application unique databases. IMS reads the TPFDD data from a Core resident OPLAN, converts it to the proper format, selects the appropriate data elements needed by the specific application, and loads the TPFDD data into the application. IMS can pickup TPFDD data from the file area of another application and move it back through the client/server communication to the Core database. The limitation of this approach is that the data will not be automatically distributed to other GCCS Core databases as would a transaction. RFM has 2 functions. One function, UPDATE retrieves the latest version of the reference file from the Core database into RFM. The other function, LOAD, copies the reference file from RFM into the application in the format required by the application.

## **APPENDIX B**

### **DO NOT REQUIRE CORE DATABASE**

GSORTS receives data sets for update into its ORACLE database from the NMCC. The AHQ can perform a query on this data through the Core database and use of SQL PLUS.

JMCIS, JDISS receive their data sets through SIPRNet and the internal addressing function. Neither of them interact with any other GCCS application.

### **EXTERNAL INTERFACES**

The systems, data bases, or applications external to GCCS are grouped by those that interoperate via transactions, via send and receive message traffic, via receive only message traffic and via use of file transfer.

### **TRANSACTIONS**

Army MOB/ODEE, Air Force COMPES, USTC GTN: These transmit transactions to and receive transactions from GCCS. The transactions are exchanged between the GCCS and the CINC/Service systems using TDS interface.

Army MOB/ODEE, receives transactions from GCCS that contain information on OPLAN forces (Army units) that FORSCOM must provide to the OPLAN. FORSCOM uses MOB/ODEE to update OPLANS with command approved data on active duty and reserve Army units. MOB/ODEE sends transactions to GCCS that provide detailed data on specific Army units that will support the OPLAN.

The Air Force COMPES provides a standard automated data system to capture, store, and report Air Force deployment operations, logistics and manpower data from the base level to the JCS. The OT&P part of COMPES provides a two-way transactional interface with GCCS to receive and update force requirements.

USTC GTN send Force and non-unit requirements updates as well as carriers with itinerary, allocations and manifests to the GCCS. The GTN/GCCS interface is at USTC.

### **SEND and RECEIVE MESSAGE TRAFFIC**

AMHS, E-MAIL: These send and receive message traffic from CINC/Service systems. The GCCS capability is in the COE.

AMHS handles USMTF and DD-178/175 message formats. The source of the message can be any communications center.

E-Mail messages can have attached files in binary, ASCII or graphic formats. The message can be sent outside the GCCS domain provided it contains the domain address and is routed through the

## **APPENDIX B**

SIPRNet.

### **RECEIVE only MESSAGE TRAFFIC**

JMCIS, JDISS, GSORTS: These operate in a "parent/child" receive only mode.

JMCIS can use USMTF or OTH-GOLD messages. The JMCIS parent in a CINC's headquarters receives information about the movement of vehicles, ships, planes, etc. The messages provide the "tracks" of movement for the reportable item. The tracks messages are received and written directly to the JMCIS parent database. JMCIS can forward all or selected tracks messages to child JMCIS databases for review.

JDISS uses USMTF messages. The JMCIS parent in a CINC's headquarters receives intelligence reports. The messages are accumulated into the parent database. The parent may forward all or selected messages to a child database for review on the child system.

GSORTS uses either message traffic or file transfer to move the GSORTS file from the NMCC to each GCCS site. Once at their site, the FDBM will use the GCCS RFA capability to move the GSORTS file into the Core database.

### **FILE TRANSFER**

GCCS(T), Marine Corps MAGTF II, Navy RUDRS, DMA Map data, NMCC reference files:

GCCS(T) provides OPLANS, once they are downgraded to SECRET, to GCCS for further planning and execution.

The Marine Corps MAGTF II will download on OPLAN TPFDD that contains information on OPLAN forces (Marine units) for Marine Corps planner review sourcing. The planners will update the TPFDD with command approved data on active duty and reserve Marine units. The MAGTF II will produce a TPFDD file to update the OPLAN in GCCS.

Navy RUDRS permits the Navy to update OPLANS with command approved data on active duty and reserve Navy units. A GCCS OPLAN TPFDD download is accomplished and the file is transferred to RUDRS. Likewise, RUDRS produces a TPFDD file to update the OPLAN in GCCS.

Update files containing reference data needed to assist the warrior are transferred into GCCS from the DMA and NMCC using the File Transfer Protocol. The NMCC reference files transferred are: Geo-Locations, TUCHA, PORTS, APORTS, and LFF. Once at their sites, the FDBM uses the RFA to move the reference files into the Core database. The TUCHA and Geo-Locations data also can be updated by users at their host GCCS site using the new RFA capability. The RFA will produce a separate file of data updates in UNIX that can be file transferred to all other GCCS sites. The update files can be loaded to the Core database using ORACLE SQL. The movement of changed data must be coordinated with the JNOCC.

## APPENDIX B

## **APPENDIX C**

### **REFERENCES**

GCCS Automated Information System (AIS) Security Plan for Version 2.0, May 1, 1995

GCCS Concept of Operation, DRAFT

Global Command and Control (GCC) Functional Economic Analysis (FEA), February 28, 1995

Global Command and Control System Exercise (GCCS-E), Exercise Positive Response 95-2, Draft Letter of Instruction (LOI), 7 April 1995

GCCS Evaluation Plan for GCCS Applications, October 7, 1993

GCCS Implementation Procedures for the GCCS Version 2.0, March 17, 1995

GCCS JOPES Database Implementation Strategy

GCCS Management Structure, CJCSI 6721.01

GCCS Mission Need Statement, June 8, 1995

GCCS Operational Evaluation Plan (OEP) Revision 2, May 1995

GCCS Program Management Plan, January 1995

GCCS System Administration Manual, May 12, 1995

GCCS Version Description Document for Version 2.1, June 15, 1995

JOPES Migration Assessment Plan, April 3, 1995

System Users Manual: GCCS Version 2.1, June 21, 1995

GCCS Version 3.0/3.1 EPIP, Annex C: Functional Description, May 30, 1997

## APPENDIX D

### GCCS v3.0 Functionality

- a. **Automated Message Handling System (AMHS)** provides GCCS users with the capability to work with AUTOMated DIGital Network (AUTODIN) messages, both in transmit and receive mode. AMHS also supports the ability to automatically update various databases, based upon formatted AUTODIN messages.
- b. **Common Operational Picture (COP)** capabilities are provided by the Joint Maritime Command Information System (JMCIS). Display of near real-time and datalinked air, land and sea tracks are an essential COP feature. These tracks can be displayed against Defense Mapping Agency (DMA) raster and vector maps.
- c. **GCCS Air Tasking Order (ATO) Review Capability (GARC)** provides GCCS with the ability to receive and view US Message Text Format (USMTF) ATO Confirmation (ATOCONF) messages disseminated by the Contingency Theater Automated Planning System (CTAPS).
- d. **Joint Deployable Intelligence Support System (JDISS)** is the technical baseline for the DoD Intelligence Information System (DoDIIS) client/ server environment. JDISS includes INTELINK at the Secret classification level. JDISS provides the Joint Intelligence Center (JIC), Joint Task Forces (JTF), and operational commanders with on-site automation support and connectivity to execute the intelligence mission.
- e. **Global Reconnaissance Information System (GRIS)** supports the planning and scheduling of monthly theater reconnaissance reports. GRIS is the culmination of migration of three other reconnaissance information systems. GRIS also provides monitoring capabilities.

**Planning and Execution Applications.** Time Phased Force Deployment Data (TPFDD) is used to develop plans and alternatives, as well as the execution of approved plans. This requires the automated tools and activities described below.

- a. **Joint Operational Planning and Execution System (JOPES) Navigation (JNAV)** is a graphical system level navigation application that allows users to easily start GCCS applications and switch between them. These include:
  - (1) **Requirements Development and Analysis (RDA)** allows editing of TPFDDs and graphical analysis of Courses Of Action (COAs) with respect to TPFDD modifications. RDA also provides a capability for creating and modifying force and non-unit requirements associated with Operations Plans (OPLANs).

## APPENDIX D

- (2) **Scheduling and Movement (S&M)** handles C2 information on deployment activity and status. S&M tracks and reports on TPFDD requirements. S&M allows GCCS users to work with Transportation Component Command (TCC) carrier and organic movement data before and during deployment. S&M can provide carrier support for more than one OPLAN. S&M allows user Ad Hoc Queries (AHQs).
- (3) **Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE)** uses logistics related attributes, such as unit consumption factors, to calculate time-phased requirements for non-unit related supplies. LOGSAFE can receive data from Joint Engineer Planning and Execution System (JEPES). Strategic movement requirements can be grouped to optimize lift needs.
- (4) **Joint Flow and Analysis System for Transportation (JFAST)** allows GCCS users to rapidly analyze a COA for deployment and sustainment. JFAST also provides the ability to generate changes to Force Modules.
- (5) **Joint Engineer Planning and Execution System (JEPES)** provides GCCS users with a capability to determine requirements and adequacy of engineering support provided in OPLAN COAs. JEPES allows planners to develop the Civil Engineering Support Plan (CESP) for an OPLAN. Using pertinent TPFDD data, JEPES can compute facility requirements and determine if adequate facilities exist to support deployed forces.
- (6) **Global Status Of Resources and Training System (GSORTS)** is an output application providing status and location of unit data, from the Status Of Resources and Training System (SORTS) database. Unit location can be plotted onto DMA digital map products. GSORTS currently uses all defined Joint data elements and contains all Service unique elements. GSORTS allows data retrieval by category of unit, type of unit, specific unit and by OPLAN.
- (7) **Ad Hoc Query (AHQ)** is part of S&M. AHQ allows OPLAN end users to query S&M on scheduling and movement requirements for a given OPLAN. A toolkit allows users to build queries and reports, thus minimizing need for specialized knowledge of the database.
- (8) **Information Resource Management (IRM)** is a generalized JOPES core database management subsystem. IRM provides the capability to load, modify, manipulate, and delete OPLAN data. OPLAN access, privileges and auditing are managed through IRM. IRM is also referred to as System Services (SYS SVC).

**Mission Support Applications.** GCCS, Version 3.0 currently provides three mission support applications, listed below. As the DoD mission support applications are integrated into the DII, they will become available to GCCS users, as appropriate.

## APPENDIX D

- a. **Airfields** provides GCCS users with comprehensive information on over 40,000 free world airfields. This information is supplied by the Defense Mapping Agency Aerospace Center (DMAAC). Reports provide one line summaries for each listed airfield. The database is updated monthly.
- b. **Evacuation File Maintenance and Retrieval System (EVAC)** is a JS and State Department automated computer database and retrieval system used to identify the number of potential evacuees located at each reporting foreign service post worldwide. Retrieval is allowed by country and districts within a country. Information is received from AF77" reports from the AMHS.

**Common Operating Environment (COE) Support Applications.** COE Support Applications provide four user services, listed below. The primary objective is to furnish, generic, COTS based information transfer services to the GCCS user community and their applications.

- a. **Office Automation** is supported by a suite of Applixware COTS products, including Applix Words, Applix Spreadsheets, Applix Mail, Applix Power Brief and Applix Ovation. The latter is a presentation application that communicates with DOS based systems.
- b. **Teleconferencing (TLCF)** Two applications provide GCCS users with teleconferencing functions. A third application provides a World Wide Web information search and retrieval capability.
  - (1) **Internet Relay Chat (IRC)** is a chatter style application that allows multiple users to participate in conferences. Several types of channels, with varying degrees of privacy, can be established.
  - (2) **Internet News** provides access to a bulletin board style broadcast service. Articles posted to the bulletin board are arranged by newsgroups. Various functions are supported, including the ability to trace a subject through a series of articles within a newsgroup and send correspondence to article authors.
  - (3) **World Wide Web (WWW)** browser service is provided through Netscape. The GCCS user may retrieve information through queries or links to other documents or websites.
- c. **TELNET** provides the GCCS user with the ability to log-in and use the application resources of any server across the network. The principal function of TELNET is to initiate text based or X-Windows applications, which, because of application design or security, must be executed from a specific server instead of from the user's local hardware

## APPENDIX D

- d. **File Transfer Protocol (FTP)** is used to directly control the transfer of files to and from a distant server. FTP is especially useful in transferring large files and is recommended when e-mail attachments exceed 500K bytes.

## **APPENDIX E**

### **Year 2000 Certification Plan**

#### **I. INTRODUCTION**

1.1 The JITC Year 2000 (Y2K) Compliance Certification Plan provides the instructions for determining compliance of information technology, software and systems that face the "Y2K challenge." The "Y2K challenge" is the term used to describe the potential failure of information technology (IT) prior to, on or after January 1, 2000. This potential exists because of the widespread practice of using two digits, not four, to represent the year in IT systems. The problem is exacerbated by the practice of using date fields as indexes and other non-date related applications. The associated but unrelated calendar anomaly that must be included in Y2K systems repairs is the fact that Y2K is a leap year unlike most other centuries.

1.2 For clarification on the requirement, the mandates, certification and reporting. The following references are provided:

Memo, 3 May 1996, DISA/CV (Kelley), "b. All systems that rely on date-intensive operations must be the primary focus of our fix efforts. These systems--especially if mission critical, C2, messaging, financial or personnel systems--must be certified as year 2000 compliant no later than 1 October 1997.

DISA Y2K Management Plan, DISA/CIO, 20 Nov 1996, Paragraph 3.a. "Mission critical systems. Systems that organizations determine as critical to their operations and functions and especially those systems that are command and control, messaging, financial, or personnel. Systems using date elements for date-intensive calculations, sorts, merges, and controls must be the first priority for year 2000 compliance certification and must be fixed not later than 1 October 1997."

Memo, Joint Staff Priorities, FY97 Spend Plan guidance, "Priority #4, Identify and correct "Year 2000" automated systems failure problems in GCCS."

DOD Year 2000 Management Plan, OSD/C3I (Paige), Version 1.0, April 1997, Paragraph 4.4, Page 5: "The DOD target for completing of all Y2K efforts is November 1, 1999. However, it is expected that most systems will be compliant well before this date." Paragraph 5.4.8, page 18: "Acceptance testing should be completed no later than June 30, 1999." Paragraph 8.4 Phase III (Renovation), "Required system "fixes" are accomplished, target completion date Dec 1998. Confirmed by January 1999."

Memo, 25 April 1997, DOT&E Director (Coyne), Year 2000 Data Processing Problem, "The Year 2000 compliance status of a system will be reported in the OT&E report."

## **APPENDIX E**

Msg, 30 April 1997, DISA/CC (Edmonds), "all, repeat all DISA systems will be tested by JITC for Y2K compliance before we certify that they are.... No new system or application will be allowed in the DII infrastructure that has not been tested and certified as compliant."

### **II- PURPOSE AND SCOPE**

#### **2.1 Purpose**

The JITC GCCS Y2K Compliance Certification Plan provides the steps necessary to ascertain if GCCS systems have been designed to ensure a non-impact transition from the 20th century to the 21st century. This will include the correct identification of the year 2000 as a leap year. Those systems deemed properly modified will be certified Y2K compliant. Systems not compliant (neither compliant to the standard eight digit date format and/nor vulnerable to transition to the "00" year) will be identified and reported accordingly.

#### **2.2 Scope**

This Plan applies to all systems, subsystems, applications, and segments contained in the GCCS supported by information technology, technical environment, and communications devices. Information technology support includes hardware, firmware, commercial off the shelf (COTS), Government off the shelf (GOTS) developed software, and data. Software includes COTS/GOTS packages, operating systems, third and fourth generation language compilers and interpreters, functional applications, system utilities, translators, and database management systems (DBMSs). Data includes databases, files, and other data storage structures and mechanisms, data and system interfaces and interchanges, Electronic Data Interchange (EDI) transaction sets and implementation conventions, and other messages or forms of data exchange.

### **III- COMPLIANCE CERTIFICATION STRATEGY**

3.1 The basis for JITC compliance certification will include: (1) JITC's participation at all levels of GCCS testing, (2) Government performed risk assessments performed on all GCCS developer's methodology, (3) Developer's testing results, (4) Integrated Developmental/Operational testing (DT/OT) results, and (5) specific JITC-designed Y2K checks. The certification process builds from assessments and results, ensuring that Y2K engineering and management attention are committed throughout the process. Each building block increases the confidence level leading to system certification. Results and issues must be identified and tracked to resolution. Results, assessment and JITC experience will form the basis for certification.

3.1.1 JITC Participation. JITC is an active participant within the OSF and have primary responsibility with each step of the test planning and testing. The GCCS Test Program is described in the GCCS Test and Management Plan (TEMP). The test strategy largely leverages off development testing efforts broken down in three Modified Development Testing (MDT) stages: MDT#1 JITC and User involvement testing at the developer's facilities; MDT#2 JITC involvement at Operational Support Facility's (OSFs) segment acceptance testing including compliance, integration, and configuration management; MDT#3 JITC performed Acceptance

## APPENDIX E

testing at JITC and Beta test sites. The MDT is followed by the Operational Test Readiness Review and OT. As an active participant and OPR, JITC is able to gather first hand information on the maturity of Y2K. Preliminary Y2K assessments, issues, and trouble reports will be generated and tracked. These issues and resolutions will support certification conclusions.

3.1.2 Risk Assessments on GCCS Developer's Methodology. The OSF conduct on-site assessment of each developer's methodology and approach to identify and resolve Y2K issues. These assessments guide any specialized Government test cases and scenario. Products from each assessment are the developer's action plan, timeline, and the Government's risk assessment rating with comments. Assessment forms the critical information necessary to compliment Y2K engineering/management compliance.

3.1.3 Developer's testing results. As part of formal delivery of software packages, developers are required to state Y2K compliance; discrepancies, if any; description of their process to determine Y2K compliance; interfaces; and status of interface transactions compliance. This information, associated test procedures and reports, completed Y2K assessment checklist, and/or the developer's Y2K action plan support certification conclusions.

3.1.4 Developmental/Operational testing results. OSF testing and JITC conducted system level operational testing may uncover Y2K issues. The OSF will perform some Y2K specific test cases and scenarios to ensure Y2K compliance on selected (high risk, critical) applications and segments. Complaint issues generate GCCS System Problem Reports (GSPRs) which are tracked to resolution. Responsible developers are notified of abnormalities found during OSF testing. Data, test results, and resolution narratives support certification determination.

3.1.5 Specific JITC-designed Y2K checks. Final compliance certification requires a series of tests designed to detect Y2K problems at each subsystem, i.e., hardware platform, operating system and common operating environment, application software, and export/import interfaces. These tests will be target high risk or suspect non-compliant subsystems. The depth and amount of specific testing will be determined based on previous testing and inspection. As risk reduction and preparation, JITC will perform "characterization" testing on selected GCCS application/segments to assess and confirm the state of GCCS compliance.

3.2 A baseline of performance will be established by assessing data provided from all system reports. The baseline testing will be followed by tests on each subsystem designed to ascertain if the system handles the Y2K situation. Based on the outcome of these tests, analyses of the subsystems will begin to identify the exact cause of failure. Recommendations for resolution of any failures will be made. If the subsystem is COTS or GOTS, the vendor/developer will be identified and contacted for solution options.

## **APPENDIX F**

### **Considerations for Future Assessment**

#### **1. Background and Approach**

1.1 This appendix will discuss guidelines for tailoring the levels of testing to field future increments and revisions to the GCCS 3.0 baseline. This appendix is not to be prescriptive but to shape the general process by which future testing/assessment decisions will be made. Once GCCS 3.0 stage I is tested and fielded, it will provide a core block for assessing subsequent increments. The steps delineated here discuss a process which will provide reasonable confidence to the overarching assessment strategy (starting at development and proceeding through fielding) while mitigating the overall mission consequences, i.e. risk.

1.2 More specifically, this appendix provides the overall framework for the process of determining the levels of testing that are appropriate to the mission consequences of the system upgrades and revisions and describe the process by which performance can be assessed and determined. There are two major portions of this framework. The initial step is assessing mission consequences: this entails an analysis of the factors that affect the likelihood of success of an increment and an understanding of the mission impact should the increment fail. The next step is to define the amount of testing that will provide sufficient, but not unnecessary, assurance that risk will be mitigated to an acceptable level.

1.3 DISA, with JITC as the lead element, will initially perform a risk assessment of a newly proposed increment, which includes an evaluation of potential threats to success and the mission impact of failure. JITC, in coordination with the GCCS PMO, will then propose an appropriate level of testing/assessment for the new increment, which the Joint Staff must approve. (DISA/JITC will be assisted by the executive agent of the proposed increment.) JITC then will prepare the appropriate test plan/assessment(s). Once the test plan/assessment(s) are approved by the appropriate bodies, (e.g. the DOT&E had to approve the full OT needed for GCCS 3.0), the test/assessment(s) will be conducted and the appropriate report(s) issued.

1.4 The next three sections will elucidate on these general comments: characterizing risk, discussing different levels of testing, and determining measures for each increment change to the baseline.

#### **2. Risk Assessment**

2.1 This section will discuss risk but will not repeat discussions of risk in other documents (see references) which discuss risk, especially for testing. In general, there are two primary factors in assessing the risk of a system element: the likelihood of failure and the impact on the mission of an increment's failure to be operationally effective and suitable. These two components need to be evaluated only to the degree required to decide among a few distinct levels of testing. From these two evaluations, one can then assess the overall risk of a system increment.

## **APPENDIX F**

2.2 In examining the likelihood of failure, the assessor should generally evaluate the following categories: software stability and functionality; compatibility and functionality; data integrity, synchronization and recovery; security and IW protections; safety; configuration control; supportability; eventual de-installation/replacement of the software; and graceful degradation and fallback options. The assessor should examine the particular characteristics of the increment and its specific development. For each increment, not all categories will have equal importance.

2.3 Based upon these category assessments and the relative significance of each area, the assessor should make an overall evaluation of the likelihood of the increment's failure to be operationally effective and suitable. Again, the assessor should base his judgment upon the particulars of the increment, the development process and the reliability of the available data. Additionally, the assessor must use his judgment and knowledge of the program to consider other risk factors for this specific increment. Each category the assessor uses should be evaluated as accurately as possible and use the following levels of resolution as a guide: insignificant likelihood of failure, low likelihood of failure, moderate likelihood of failure, or high likelihood of failure. After each category is assessed, an overall assessment must be made.

2.4 Once the likelihood of failure is assessed, the identification and evaluation of the mission impact of increment failure must be made. The mission impact assessment should consider the impact of the possible failure on the mission of the whole system. Impacts should be assessed as either minimal (no major interference with mission accomplishment), moderate (substantial degradation of mission capabilities), or significant (malfunction causes catastrophic damage to the installed system).

2.5 Once the mission impact and the likelihood of failure of an increment have been determined, the risk assessment may be made as the product of these two elements. Generally, the mission impact should be weighted more heavily than the likelihood of failure. Proceeding from the overall risk assessment, the proper level of testing can be determined.

2.6 This overall risk determination process need not necessarily be a heavily formal process. While it must be thorough and full, it needs to be done as fast as possible so that the process itself will not hold up the testing/assessment(s) that must be done for the increment .

### **3. Levels of Testing**

3.1 JITC, in coordination with the GCCS PMO, must recommend to the Joint Staff the level of testing that most effectively provides confidence that a new increment will meet mission needs. A range of test activities should be considered and matched to the risk of the specific system increment. The range of testing for increments developed subsequent to the core (3.0) system will extend through four levels, from an abbreviated assessment to a full, conventional operational test and evaluation. The detailed design of testing activities at each level of testing must be based upon the fundamental objective of evaluating of the ability of the tested system to accomplish its mission when deployed. In pursuit of this goal, four general levels of testing are identified.

## APPENDIX F

3.1.1 Level I: Abbreviated Assessment. Level I testing is appropriate for maintenance upgrades and increments that provide only minor system enhancements, pose an insignificant risk, and can be easily and quickly removed. Key features of the abbreviated assessment are:

- a. It is essentially a developmental testing effort,
- b. Limited fielding can be permitted prior to the evaluation, and
- c. Changes can be accommodated through normal engineering change procedures

3.1.2 Level II: Alpha test. Level II testing should be applied to increments that provide only minor system improvements and present a minor risk. Such lower risk increments have only minimal potential to impact other system applications and cannot disrupt the basic system's ability to support the mission. After thorough alpha testing, an increment may be deployed to selected operational sites for additional feedback if needed prior to full fielding. Key features of the Alpha tests are:

- a. It is essentially a combined DT/OT testing effort,
- b. The assessment is based primarily upon close monitoring of selected, developmental/technical activities and upon DT results,
- c. Accelerated testing is permitted and encouraged, and
- d. A security assessment is necessary.

3.1.3 Level III: Beta test. The beta test is suitable for increments supporting modest, self-contained, system improvements that present a moderate level of risk, but are limited in the potential disruption to an installed system. Key features of beta testing are:

- a. Actual operators are at the operational sites performing real tasks,
- b. The emphasis is on assessment and evaluation,
- c. It is less formal than a full operational test, and
- d. All events shall be assessed/noted but not necessarily formally tested.

3.1.4 Level IV: Full Developmental and Operational Tests. This is the highest level of testing and the most comprehensive. The test events are carried out in a operational environment and must be approved by the appropriate agencies. Level IV testing must comply with the DoD 5000 series of regulations. This level of testing is performed when it is anticipated that the proposed increment could cause serious deterioration of current performance, possibly affect the interconnected systems in a serious manner or result in major changes in operational practices.

3.2 These levels of testing are a guideline only. Since GCCS increments will be of all types, it may be that some combination of testing/assessment between the mentioned levels is more appropriate and should be considered.

## APPENDIX F

### 4. Determining Measures

4.1 This section will detail the general process by which performance of new system increments following introduction of the GCCS 3.0 stage I baseline (e.g. new applications introduced in GCCS 3.0 stage II) could be assessed. It is assumed that for the increment to be assessed, no specific performance measures have been noted and a process needs to be delineated to do this. (If, however, performance measures - tied to functional requirements - have been provided prior to the development process, these measures shall be rigorously measured during the testing/assessment process.)

4.2 The initial step in assessing new increments will generally be at a contractor facility. (This is known as MDT stage I for GCCS 3.0. stage I.) At this phase, the tester, generally JITC, works with Subject Matter Experts (SME), to assess the increment. These assessments must trace functionality back to requirements and should use a requirements-traceability matrix. (Note: the RID identifies broad mission capabilities required by the users. From the RID and the requirements approval process identified in CJCSM 6721.01, 15 March 1997, new requirements are approved which eventually lead to the increment that is being tested.) The SME, in coordination with JITC, should designate the “must have” functions for the increment - which will be verified in later testing and must also be traceable back to noted requirements. These “must haves” then can become Measures of Effectiveness and Suitability, MES.

4.3 The JITC testers shall prepare a structured questionnaire - based on the requirements, common sense and prior experience - as a starting position to elicit from the SME their functional knowledge of the system concerning the most critical capabilities. Associated with these MES, some Minimum Acceptable Values (MAV) should be noted that the SME considers minimally acceptable. These MAV, often called “criteria for success,” are the user’s yardsticks for knowing that the requirements have been satisfactorily met. These can be a demonstrated functional capability or other means that the user/SME will apply.

4.4 The next step is for these MES and MAV to be validated by the users as appropriate and representative of the full capabilities that they need. The process of validation shall primarily be via the appropriate GCC working group. Upon completion of a nominative MDT stage I, JITC shall provide the assessment (via the GCCS PMO) to the Joint Staff, who will pass it on the appropriate working group. As soon as possible, this working group will examine this assessment, determine if the MES and MAV are valid, make comments and provide their recommendations to the Joint Staff, which will provide guidance to DISA. This process must be expedited and it is entirely appropriate if done electronically, e.g. via the WWW. The intent is to provide a response back quickly enough so that the measures could be assessed during the next stage of testing for the increment in question.

4.5 During this next stage of testing, these measures could then be assessed to determine if the increment is meeting expectations. SME and user support will be needed to advise testers concerning the potential mission consequences of new problems or violation of MAV thresholds encountered during the testing. Problems encountered will be written up by the assessor and presented for evaluation at conclusion of the testing.

## **APPENDIX F**

4.6 The process delineated should help provide a trace from the original requirements to performance evaluation that builds upon the basic steps and user participation activities already incorporated into the test program. The goal is to provide a baseline of performance for future installations and enhancements.